Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs	)	WC Docket No. 18-89

WRITTEN *EX PARTE* SUBMISSION OF HUAWEI TECHNOLOGIES CO., LTD., AND HUAWEI TECHNOLOGIES USA, INC.

Huawei Technologies Co., Ltd., and Huawei Technologies USA, Inc. (collectively, "Huawei"), by their undersigned counsel, submit this *ex parte* presentation to the Federal Communications Commission ("FCC" or "Commission") to supplement the record in the above-captioned docket with additional publicly available facts about other telecommunications companies. These companies market or may wish to market telecommunications equipment and services in the United States and have substantial connections to China. This additional information further demonstrates that the Commission's proposed approach is irrational and should not be adopted.

Huawei submits as **Exhibits 1-34** documents which, taken together, demonstrate that numerous telecommunications companies have connections with China that are equally or, in many cases, more significant than those of Huawei. Some of these companies are state-owned entities; others have substantial manufacturing or other business interests in or with China, including ties between China and the two primary providers of 5G telecommunications equipment to recipients of Universal Service Fund ("USF") support. This information highlights the irrationality and arbitrariness of premising any exclusion of Huawei from the USF program on Huawei's supposed connections with China.

As Huawei has previously explained, singling out Huawei and ZTE, when numerous other companies have ties to China, demonstrates that the proposed rule is irrational and not based on any evidence that such ties present a security risk. Indeed, regarding a company as a security risk because of connections to China smacks of the invidious discrimination barred by the Constitution's equal protection guarantee. *See* Huawei Comments 44-47 (June 1, 2018). Beyond that, the Commission's proposed rule makes no reference to a company's cybersecurity-management procedures or cybersecurity risks that can come from anywhere in the supply chain. The telecommunications supply chain is global, and all major telecommunications manufacturers have operations in China, not to mention all around the world. *E.g.*, *id.* at 39-41; Huawei Reply Comments 21-22 (July 2, 2018); Huawei *Ex Parte* Submission 38 (Aug. 6, 2018). In other words, connections with China are the inevitable result of globalization; they are not a proxy for national security threats. The Commission appears to have recognized as much in other ways. For instance, the Commission has not targeted Nokia, even though Nokia (unlike Huawei) has formed a joint venture with the Chinese government. Huawei Comments 40; Huawei Reply Comments 21. That is *not* to say that the Commission should target Nokia—only that the Commission's approach is arbitrary and not based on any evidence. And even if there *were* some reason to suspect a security risk, that would not justify singling out Huawei and a handful of other companies.

The proposed rule may rest on the assumption that Chinese law or the Chinese Communist Party may require companies to spy for the Chinese state. As an initial matter, such reasoning provides no reason to single out Huawei. More importantly, though, the notion is false. As Huawei's experts have repeatedly explained, Chinese law does not permit the Chinese government to require Chinese telecommunications companies to cooperate with China's government to engage in espionage and cyberattacks. *See* Huawei Comments 43, 87-89; *id.* Ex. D (Declaration of

Ariel Lu Ye); *id.* Ex. E (Declaration of Jihong Chen & Jianwei Fang); Huawei Reply Comments 64; Huawei *Ex Parte* Submission 14-20, 36-47 (Aug. 6, 2018); Huawei *Ex Parte* Submission Ex. B (Aug. 6, 2018) (Supplemental Expert Report of Jihong Chen & Jianwei Fang); Huawei *Ex Parte* Submission & Attach. A (May 10, 2019) (Expert Report of Dr. Hanhua Zhou). Nor are Chinese companies beholden to the Communist Party. Much to the contrary, the Chinese state is bound to respect their autonomy. *See* Huawei *Ex Parte* Submission Ex. A (Aug. 6, 2018) (Expert Report of Jacques deLisle). And that makes good sense. As Huawei's expert has explained, the Chinese government would jeopardize its high-priority economic agenda by attempting to coerce leading companies like Huawei to spy for it. *Id.* at 12. For its part, Huawei too has overwhelming economic incentives to compete vigorously in the global market for telecommunications equipment and services free from any taint of complicity in state espionage efforts. *See, e.g.*, Huawei Comments Ex. L, at 10-12 (J. Suffolk, *Cyber Security Perspectives* (2012)).

Additionally, attached as **Exhibit 35** is a report regarding supply chain vulnerabilities prepared by Interos Solutions, Inc., for the U.S.-China Economic and Security Review Commission of the U.S. Government ("Interos Report"). The Interos Report identifies fifteen "entities of concern" with "relation[s] to the Chinese government" that the report claims pose supply-chain risks to U.S. information networks. The report further identifies several companies who are important suppliers of Dell and Microsoft—but not Huawei—as "present[ing] the most risk to the supply chain" as a result of their "close ties to Chinese government entities, particularly entities involved in China's military, nuclear, or cyberespionage programs."

Huawei stresses that it does not agree with the assumption by the authors of the Interos Report that substantial relationships with Chinese entities constitute any security risks to the telecommunications networks of other countries, and Huawei strongly denies any allegations—which

the report concedes are based on "unconfirmed reports"—about intellectual property theft. Huawei also does not agree with any of the other assertions about Huawei that appear in the Interos Report.

The point, rather, is that any suggestion that the U.S. Government—including the Commission—can solve supply chain issues by singling out a small number of companies for punitive treatment is profoundly misguided and will be entirely ineffective. The report demonstrates that the Commission's proposed rule is based on speculation and innuendo, not evidence.

As Huawei has previously argued, in ignoring the substantial Chinese connections of other telecommunications companies, the Commission has proposed a rule that relies on speculation, innuendo, and false assumptions rather than the realities of the global supply chain. Consequently, the proposed rule would not only punish Huawei for no reason, but it would also render the Commission's proposed rule ineffectual in achieving its stated goals of enhancing the security of the telecommunications supply chain.

Respectfully submitted,

/s/ Andrew D. Lipman

Andrew D. Lipman
Russell M. Blau
David B. Salmons

MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Ave., NW
Washington, D.C. 20004
(202) 739-3000
(202) 739-3001 (Fax)
andrew.lipman@morganlewis.com
russell.blau@morganlewis.com
david.salmons@morganlewis.com

Counsel to Huawei Technologies Co., Ltd., and Huawei Technologies USA, Inc.

Glen D. Nager
Bruce A. Olcott
Ryan J. Watson

JONES DAY
51 Louisiana Ave., NW
Washington, D.C. 20001
(202) 879-3939
(202) 626-1700 (Fax)
gdnager@jonesday.com
bolcott@jonesday.com
rwatson@jonesday.com

September 18, 2019

EXHIBIT LIST

Exhibit 1: "Company Profile" of Panda Electronics Group Co. Ltd.

Exhibit 2: Ericsson's "About Us: China" Webpage

Exhibit 3: "Ericsson Preserves Competitiveness on 5G Development in China"

Exhibit 4: "Ericsson: Things are Getting Better"

Exhibit 5: Excerpts from LM Ericsson Telephone Co.'s Form 20-F Annual Report for Fiscal Year Ended December 31, 2018

Exhibit 6: Excerpts from Nokia Corp.'s Form 20-F Annual Report for Fiscal Year Ended December 31, 2018

Exhibit 7: Excerpts from Nokia Corp.'s Form 20-F Annual Report for Fiscal Year 2017

Exhibit 8: Excerpts from China Mobile Ltd.'s Form 20-F Annual Report for Fiscal Year 2018

Exhibit 9: "FCC Denies China Mobile's Bid to Provide International Telecom Services in the U.S."

Exhibit 10: "Company Overview" of China Telecom (Americas)

Exhibit 11: Excerpts from China Telecom Corp. Ltd.'s Form 20-F Annual Report for Fiscal Year 2018

Exhibit 12: Excerpts from China Unicom (Hong Kong) Ltd.'s Form 20-F Annual Report for Fiscal Year 2018

Exhibit 13: "Nokia Corp., Nokia and China Huaxin Sign Definitive Agreements for Creation of New Nokia Shanghai Bell Joint Venture"

Exhibit 14: "Finnish Visit to Nokia Shanghai Bell"

Exhibit 15: "NSA Concerns Give Chinese Server Maker a Boost"

Exhibit 16: PC Magazine's Online Product-Overview Page for Cisco Systems, Inc.'s Catalyst 3650-48P Layer 3 Switch

Exhibit 17: Excerpts from Cisco Systems, Inc.'s Form 10-K Annual Report for Fiscal Year Ended July 30, 2016

Exhibit 18: Excerpts from Hewlett Packard Enterprise Co.'s Form 10-K Annual Report for Fiscal Year Ended Oct. 31, 2018

Exhibit 19: "Magic Quadrant for LTE Network Infrastructure"

Exhibit 20: Excerpts from Lenovo Group Ltd.'s 2017/18 Annual Report

Exhibit 21: "USA Smartphone Market Share: By Quarter"

Exhibit 22: "DoD Issues Cybersecurity Warning Against Lenovo Computers, Handheld Devices"

Exhibit 23: Backgrounder, Alcatel-Lucent Enterprise

Exhibit 24: Alpha Networks, Inc.'s "Design Manufacturing, Service (DMS)" Webpage

Exhibit 25: Alpha Networks, Inc.'s "About Alpha" Webpage

Exhibit 26: Excerpts from Arista Networks, Inc.'s Form 10-K Annual Report for the Fiscal Year 2018

Exhibit 27: Excerpts from Extreme Networks, Inc.'s Form 10-K Annual Report for the Fiscal Year Ended June 30, 2018

Exhibit 28: Excerpts from Juniper Networks, Inc.'s Form 10-K Annual Report for the Fiscal Year Ended Dec. 31, 2018

Exhibit 29: "OnePlus Breaks Into Top 5 Premium Phone Makers in US Market"

Exhibit 30: "Who is BBK, The World's Third Largest Phone Manufacturer?"

Exhibit 31: "Meet the 'Godfather' of China's Smartphone Industry"

Exhibit 32: "China's Tsinghua Unigroup to Build $30 Billion Memory-Chip Factory in Nanjing"

Exhibit 33: Tsinghua Holdings Co. Ltd.'s "Products and Technological Services" Webpage

Exhibit 34: "Shenzhen Government Takes Control of China's Leading Chip Maker Tsinghua Unigroup"

Exhibit 35: "Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology" by Interos Solutions, Inc.

Exhibit 1

"Company Profile" of Panda Electronics Group Co. Ltd.

Click to enable Adobe Flash Player

+ About Panda
Company Profile
Address From Chairman

+ Company Profile

Panda Electronics Group Company Ltd. (Panda Group) is a large comprehensive state-owned electronics enterprise with a history of over 70 years. Its business covers multiple industries including modern communications, digital audio/video and smart electronics system, electronics equipment and electronics manufacturing. Founded in 1936 and regarded as the cradle of China's electronics industry, Panda is the backbone enterprise of CEC (China Electronics Corporation).

As a key high-tech state enterprise, the Panda Group has made great contributions to national defense and modernized construction. It has been one of the top 500 enterprises for 24 consecutive years and ranked high in the top 100 electronics and IT enterprises as well as in the top 100 software enterprises. Panda brand is approved as the national famous trademark by the State Administration for Industry & Commerce of the People's Republic of China. In 1996, Nanjing Panda Electronics Company Ltd., owned by the Panda Group holding company was listed separately in the Shanghai and Hong Kong Stock Exchanges, making Panda Group the first dual-listed company in Chinese electronics industry.

Since the 1950s, more than 30 government leaders such as Mao Zedong, Deng Xiaoping, and Jiang Zemin have inspected the company, showing the sincere care and ardent hope for the development of the Panda Group. Hu Jintao, general secretary of the Central Committee of the Communist Party of China, inspected Panda Group in April, 2004, and deeply encouraged the staff to make Panda a world famous brand.

The Group has been long engaged in the innovation of core technologies with independent intellectual property rights. It has great strength in system integration and research & development in the fields of wireless communications, digital audio/video and smart information technology. It has seven national high-tech enterprises, five national engineering R&D laboratories, one post-doctoral work group and ten new product research centers. Leading science and technology personnel are developing a high standard of innovations at national and provincial institutes such as the Mobile Satellite Communication Engineering Center, the Digital Audio/Video Engineering Center, Manufacture Technology Development Center, Technology Center, Jiangsu Research Center of Optical Communication Engineering & Technology, Jiangsu Research Center of Short Wave Communications Engineering & Technology, and Jiangsu Research Center of Mobile Communication Engineering & Technology.

Panda has formed a new structure focusing on modern communications; new generation digital broadcast television and smart system equipment. With strong R&D and manufacturing capability in wireless communication field ranging from network integration and applications to terminal equipment, the Group is the national communication high-tech R&D center and an important industrial base.

In the field of civil electronics, Panda Group leads the market in providing first class domestic special communication equipment, and automatic fare collection systems, combining independent development with international cooperation. It has developed mobile communication systems including mobile communication network equipment, specific communication terminals, emergency communication and vehicular communication products, ACC/AFC rail traffic system solutions and equipment, and complete equipment for automatic mass production. With its advantages in core technologies, key processes and high-end human resources, Panda has gained increasing competitiveness.

Panda Group is also one of the largest electronics manufacturers in eastern China. With strength in manufacturing fields such as SMT, injection molding, packing, precision molding, sheet metal and digital precision mechanical machining, it provides SMT, auto-insertion of PCBs and PCBA assemblies, as well as installation, testing and maintenance services. With more than 20 advanced SMT production lines, the company has an annual production capacity of more than 15 million digital chassis and assemblies, plus over 10 billion components, 6 million LCD sets, PDP modules and complete color TVs. Panda Electronics now produces specialized plastic moldings and profiles including spray painting and auxiliary assembling. It possesses nearly 100 injection-molding machines with clamping force from 100T to 2800T.

The main joint ventures of our company are: Nanjing Ericsson Panda Communication Co., Ltd., Beijing SE Potevio Mobile Communication Co., Ltd., Nanjing Thales Panda Transportation System Co., Ltd., Nanjing LG Panda Electrical Appliance Co., Ltd. and Shenzhen Jinghua Electronics Co., Ltd.

During the period of 'The Eleventh Five-Year-Plan', the company's accumulated turnover reached RMB 130 billion and the profit and tax reached 6.8 billion, with a 22% annual sales growth rate. Its global users are up to

Joint Ventures &Trade Links
Select.....
Panda Website Links
Select.....

90 million.

Exhibit 2

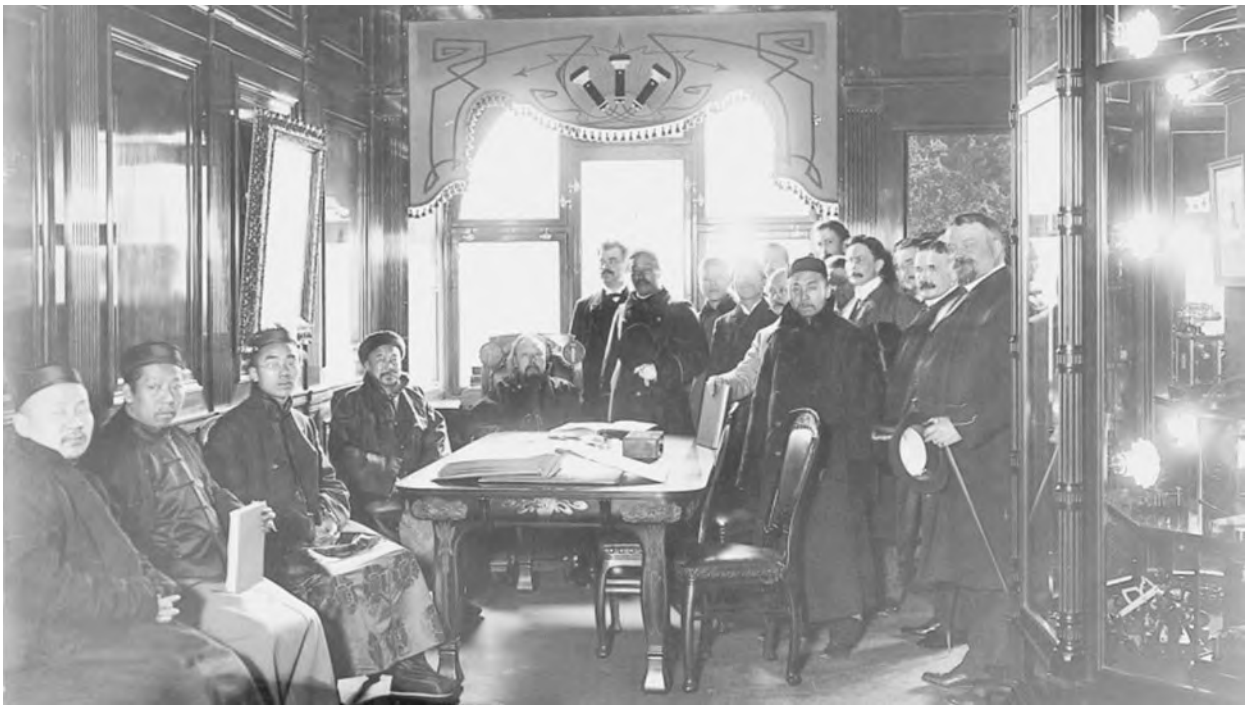
Ericsson's "About Us: China" Webpage

ERICSSON

- Home
- About us
- Ericsson history
- Places
- China

History |

China



Ericsson had already established a presence in China in the early 1890s through the telephone sales of Gustaf Öberg in Shanghai. Orders increased after the turn of the century when Öberg became president of a telephone operating company in the city. In 1913, Ericsson supplied equipment for a telephone station in Guangzhou (Canton). A few years later, the company also hoped to win the telephone concession in the city, but

World War I put a stop to these plans. Attempts were made again after the war but without success.

Many years would pass before Ericsson established operations in China. After the birth of the People's Republic of China in 1949 and until the death of Mao Zedong in 1976, the market was closed to Ericsson. In the late 1970s, however, the ruling Communist Party slowly began to open the enormous country to foreign companies.

At this time, Ericsson began sales of AXE stations to China. In 1985, the first representation office was opened in Beijing, and two years later, China signed what was its largest-ever telecom contract at the time for 200,000 lines of AXE.

But it was only in 1994, when Ericsson established its local company, Ericsson China Ltd, that things really took off. Just three years later, China was Ericsson's largest market with respect to order bookings.

Ericsson has several joint venture companies in China, including production companies, since the Chinese government demands local manufacturing. One important company is Nanjing Ericsson Communication Company Ltd., which was established with the electronics manufacturer Nanjing Panda Electronics. Nanjing Ericsson's accomplishments include the launch of an inexpensive mobile phone under the Panda brand that was specially developed for the Chinese market.

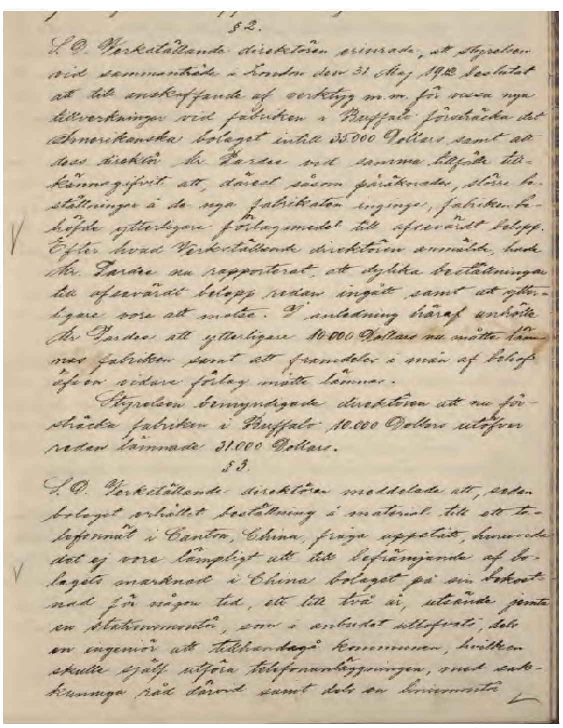
Ericsson has also invested heavily in research and training in China, which not only has its own benefits, but also provides a competitive advantage. In Shanghai, the Ericsson Communication Software Research and Development Center was established in 1997. In the same year, the Ericsson China Academy was founded in Beijing. Some 30 students are admitted each year for a two-year part-time program leading to a Master's Degree in business administration with a focus on infocom companies. Ericsson's training center in Beijing also offers shorter courses for Ericsson employees and customers.

Ericsson is assisting China in the transition from the existing digital mobile network to third-generation mobile systems. In 1999, Ericsson and the China Academy of Telecommunications Technology opened a research and development center for WCDMA technology. Together with the Beijing Institute of Technology, Ericsson has opened a research center for mobile communication.

Ericsson is particularly strong in mobile communications in China, with nearly half the market for mobile systems. With respect to fixed networks, the company's market share is about ten percent.

Author: Mats Wickman

Captain Gustaf Öberg. One of the medals is Chinese.



§ 2.

T. F. Verkställande direktören erinrade, att Styrelsen vid sammanträde i London den 31 Maj 1912 beslutat att till anskaffande af verktyg m.m. för vissa nya tillverkningar vid fabriken i Buffalo förstråcka det Amerikanska bolaget intill 35.000 Dollars samt att dess direktör Mr Pardee vid samma tillfälle tillkännagifvit att, därest såsom påräknades, större beställningar å de nya fabrikaten inginge, fabriken behöfde ytterligare förlagsmedel till afsevärdt belopp. Efter hvad Verkställande direktören anmälde, hade Mr. Pardee nu rapporterat, att dylika beställningar till afsevärdt belopp redan ingått samt att ytterligare vore att motse. I anledning häraf anhölle Mr Pardee att ytterligare 10.000 Dollars nu måtte lämnas fabriken samt att framdeles i mån af behof äfven vidare förlag måtte lämnas.

Styrelsen bemyndigade direktören att nu förstråcka fabriken i Buffalo 10.000 Dollars utöfver redan lämnade 31.000 Dollars.

§ 3.

T. F. Verkställande direktören meddelade att, sedan bolaget erhållit beställning å material till ett telefonnät i Canton, China, fråga uppstått, huruvida det ej vore lämpligt att till befrämjande af bolagets marknad i China bolaget på sin bekostnad för någon tid, ett till två år, utsände jemte en stationsmontör, som i anbudet utlofvats, dels en ingeniör att tillhandagå kommunen, hvilken skulle själf utföra telefonanläggningen, med sakkunniga råd däruti samt dels en [illegible]

https://www.ericsson.com/en/about-us/history/places/asia/china

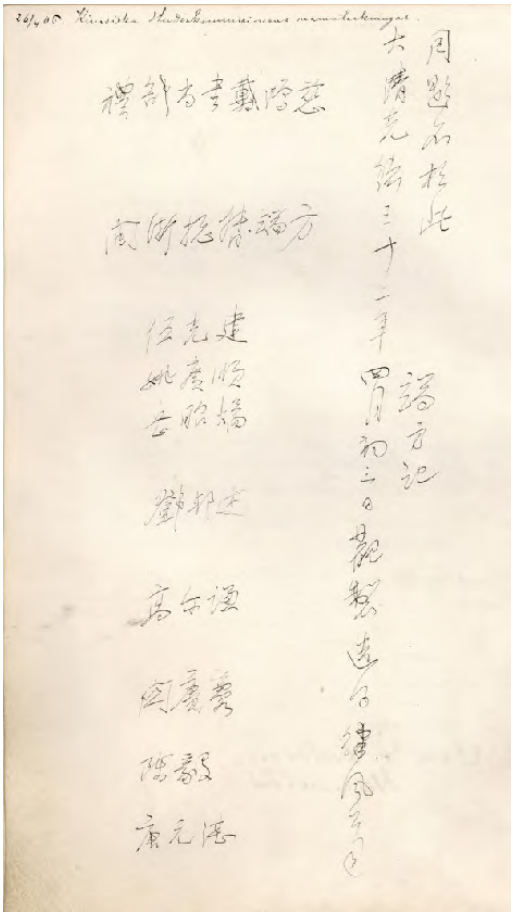
§2: The board approves a loan of USD 10,000 to the plant in Buffalo, USA.

Lars Ramqvist watching over the microscope examination of micro chips. At the inauguration of Ericsson Simtek Electronics.

Captain Gustaf Öberg dressed in Chinese clothing

https://www.ericsson.com/en/about-us/history/places/asia/china

From "The Second Better Homes and Chinese Industries Exhibition" in Shanghai, 1937. Ericsson sharing a stand with SKF, the Swedish manufacturer of ball bearings.



https://www.ericsson.com/en/about-us/history/places/asia/china

Contribute to this article

Contact info/About the site

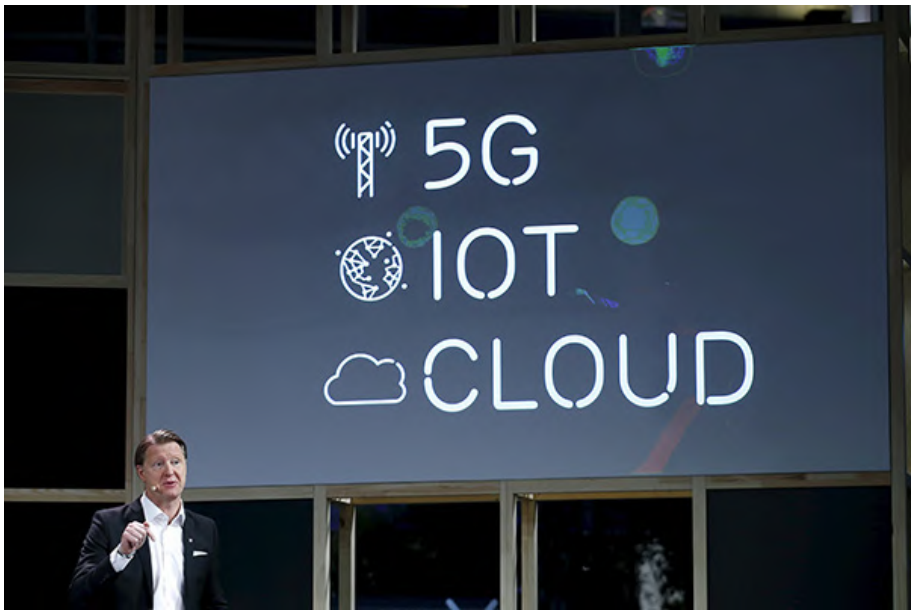
Exhibit 3

"Ericsson Preserves Competitiveness on 5G Development in China"

Ericsson preserves competitiveness on 5G development in China

By Liu Zheng in Barcelona, Spain (chinadaily.com.cn)

Updated: 2016-02-23 16:01



Ericsson's President & CEO Hans Vestberg attends a news conference during the Mobile World Congress in Barcelona, Spain February 22, 2016. [Photo/Agencies]

China is a strong foothold for Ericsson's research and development, manufacturing and services activities worldwide, company executive said.

"The core-competitiveness for Ericsson on 5G solutions in a market like China is that we have a full system view and we have a strong offering, consisting of both products and services, everything from the access, the transport, the cloud technologies and the complete management on the acquisition," Sara Mazur, vice president and head of Ericsson Research, told chinadaily.com.cn.

At MWC (Mobile World Congress), Ericsson President and CEO Hans Vestberg said the company has agreements with 20 major operators around the world to work together on 5G – more than any other vendor.

Vestberg pointed out that 5G radio test-bed field trials will start this year and the company is active in aligning industry time plans (3GPP, ITU-R) to assure the commercial launch of 5G in 2020.

Most Viewed Today's Top News

Top 10 most popular online shopping sites in China

Top 10 Chinese internet companies in 2017

Top 14 most powerful female billionaires in the world

Top 10 robotics companies in the world

Top 10 trading partners of the Chinese mainland

Top 10 luxury goods companies in the world

World leading internet sci-tech achievements released in Wuzhen

Top 10 most-used currencies in the world

Top 10 Chinese-listed companies with biggest brand value

Top 10 degrees that provide highest paid jobs in UK

Hot Topics

Fiat SpA Peugeot SA Taxi app

Internet finance Housing price

Disneyland 12306.cn WeChat

CHINADAILY FORUM

Daily life in Sri Lanka

Tulips in bloom in Jilin

Harmony in diversity? What does it mean?

Forest fire still burning in SW China

E China sees rare scene of dolphin group

Chinese father donates part of intestine to son

Is salary still the motive for overseas study?

Editor's Picks

Top 10 most Internet-savvy banks in China

Ericsson's 4G networks have been broadly deployed on a global scale in North and South America, the Asia Pacific region, the Middle East and Europe. To capture the next-generation ultra-faster 5G market, the vendor has ramped up research and development investments.

Ericsson's 5G wireless prototypes have taken shape, and the vendor has cooperated with major operators in Sweden, the United States, Japan, Korea and Brazil to test its 5G technology.

According to a company statement, Ericsson's annual R&D investment in China exceeds $310 million. With nearly 5,000 employees in Beijing, Shanghai, Guangzhou, Nanjing, Chengdu and Shenzhen actively engaged in R&D and product development of the entire Ericsson portfolio, China has become the largest and a truly global R&D base for Ericsson worldwide outside Sweden.

Currently, Nanjing Ericsson Panda Communication Co Ltd has grown into Ericsson's largest supply and manufacturing hub, supporting the company's global supply network and providing products for GSM, WCDMA, LTE and TD-LTE to more than 100 countries.

Ericsson is also working closely with the Chinese government, academia and the entire ecosystem in China to drive the global standardization of 5G.

On Dec 21, the company and China Mobile Research Institute (CMRI) signed a Memorandum of Understanding (MoU) to collaborate on 5G research and development.

The agreement will help drive innovation and early application of 5G mobile network technology in the country.

Under the terms of the MoU, which will initially cover a five-year period, Ericsson and China Mobile will cooperate in verification, trial and standardization of a new 5G Air Interface for commercial deployment from 2020.

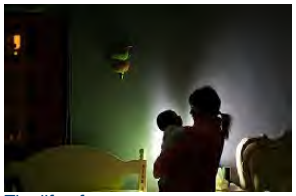
It also will closely interwork between 5G and the evolution of LTE, as well as innovate RAN features to support future industrial use cases and demonstrate, verify and conduct trials of narrowband IoT (NB-IoT) for massive machine-type communication, as well as collaboration on corresponding vertical use cases.

8.03K

Related Stories

- Ericsson reports rising income, vowing to build 5G leadership
- Empowered by vision of a connected world
- Ericsson aims big in China market: top executive
- Ericsson reports rising sales in Q2, buoyed by China market
- 5G to become available by 2020: Ericsson

Photo


The life of a yuesao


Top 10 most Internet-savvy banks in China


Candidates do squats, sing and dance to become train attendants


Top 10 loss-making Chinese companies


Top 5 smart wearable vendors in the world


Top 10 overseas destinations for Chinese tourists for the holiday

Specials


World Robot Conference 2015


Made in China - fight against counterfeit goods


2015 Beijing Forum for Emerging Markets

Exhibit 4

"Ericsson: Things are Getting Better"

5G

Ericsson: Things are getting better

by Mike Dano | Nov 8, 2018 11:34am

Ericsson raised its 2020 sales targets. (Monica Alleven/Fierce Wireless)

Ericsson raised its 2020 sales targets due to what the company said was an improving outlook for its sales of wireless network equipment.

"With our focused strategy we have created a strong foundation of stability and profitability," Ericsson CEO Börje Ekholm **said in a statement**. "Our strengthened portfolio and competitive cost structure have enabled us to grow in the third quarter of 2018, for the first time since 2014, on a constant currency basis, despite headwind from exited contracts and businesses. As the industry moves to 5G and IoT we are now preparing to take the next step to generate profitable growth in a selective and disciplined way."

Specifically, **as noted by Reuters**, Ericsson raised its net sales goal to between $23.3 billion and $24.4 billion. The company also stuck to its target for operating margins to rise above 10% in 2020, excluding restructuring. Ericsson, though, said its longer term goal of boosting operating margins to greater than 12% would occur no later than 2022.

Ericsson said growth in its networks business "is expected to come from a stronger market, selective market shares gains, and expansion of the product portfolio into close adjacent markets. In 2019, investments in 5G trials will continue. The operating margin target for 2020 is unchanged at 15% – 17%," the company said.

Ericsson is the top provider of wireless network equipment in the United States in terms of market share, **according to research firm Dell'Oro Group**, and is listed as a major vendor for all of the country's nationwide wireless providers. And Ericsson is working to stamp out new customers as well, recently having signed network-build-out agreements with the likes of **Dish Network** and **Ligado**.

Ericsson's news also comes shortly after the company **reported** its first profitable quarter since June 2016—and after the company laid off roughly 22,000 employees. The company said net sales in North America, the company's biggest regional market behind Europe, jumped 21% year over year during the quarter and network equipment sales increased 24% in North America during the same period.

Ericsson, along with rival Nokia and other telecom equipment providers, is pinning most of its hopes on 5G, a network technology that most of the world's telecom operators hope to deploy in some fashion in the coming years.

Read More On

5G Ericsson

Suggested Articles

Wireless

CBA supports content companies' requests for C-Band safeguards

by Monica Alleven
May 15, 2019 5:03pm

Exhibit 5

Excerpts from LM Ericsson Telephone Co.'s Form 20-F Annual Report for Fiscal Year Ended December 31, 2018

Table of Contents

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 20-F

☐ **REGISTRATION STATEMENT PURSUANT TO SECTION 12(b) OR (g) OF THE SECURITIES EXCHANGE ACT OF 1934**

OR

☒ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the Fiscal Year Ended December 31, 2018

OR

☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

OR

☐ **SHELL COMPANY REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

Commission file number 000-12033

TELEFONAKTIEBOLAGET LM ERICSSON
(Exact Name of Registrant as Specified in its Charter)

LM ERICSSON TELEPHONE COMPANY
(Translation of Registrant's name into English)

Kingdom of Sweden
(Jurisdiction of incorporation or organization)

SE-164 83 Stockholm, Sweden
(Address of principal executive offices)

Jonas Stringberg, Vice President, Head of Financial Control and Business Services
Telephone: +46 10 716 53 20, jonas.stringberg@ericsson.com
SE-164 83 Stockholm, Sweden
(Name, Telephone, E-mail and/or Facsimile number and Address of Company Contact Person)

Securities registered or to be registered pursuant to Section 12(b) of the Act:

Title of Each Class	Name of Each Exchange on which Registered
American Depositary Shares (each representing one B share)	The NASDAQ Stock Market LLC
B Shares *	The NASDAQ Stock Market LLC

* Not for trading, but only in connection with the registration of the American Depositary Shares representing such B Shares pursuant to the requirements of the Securities and Exchange Commission.

Securities registered pursuant to Section 12(g) of the Act:

None

Securities for which there is a reporting obligation pursuant to Section 15(d) of the Act:

None

Indicate the number of outstanding shares of each of the issuer's classes of capital or common stock as of the close of the period covered by the annual report:

B shares (SEK 5.00 nominal value)	3,072,395,752
A shares (SEK 5.00 nominal value)	261,755,983
C shares (SEK 5.00 nominal value)	0

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ☒ No ☐

If this report is an annual or transition report, indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934. Yes ☐ No ☒

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically, if any, every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T (§ 232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit such files) Yes ☐ No ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer or an emerging growth company . See the definitions of "large accelerated filer" and "accelerated filer" and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large accelerated filer	☒	Accelerated filer	☐
Non-accelerated filer	☐	Emerging growth company	☐

If an emerging growth company that prepares its financial statements in accordance with U.S. GAAP, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Indicate by check mark which basis of accounting the registrant has used to prepare the financial statements included in this filing:

☐ U.S. GAAP	☒	International Financial Reporting Standards as issued by the International Accounting Standards Board	☐	Other

If "Other" has been checked in response to the previous question, indicate by check mark which financial statement item the registrant has elected to follow.

Item 17 ☐ Item 18 ☐

If this is an annual report, indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ☐ No ☒

Company	Reg. No.	Domicile	Percentage of ownership	Par value in local currency, million	Carrying value, SEK million
Teleric Pty Ltd.		Australia	100	20	100
Ericsson Ltd.		China	100	2	2
Ericsson (China) Company Ltd.		China	100	65	475
Ericsson India Private Ltd.		India	67[3]	364	82
Ericsson India Global Services PVT. Ltd		India	100	291	51
Ericsson Media Solutions Ltd		Israel	100	9	51
Ericsson-LG CO Ltd.		Korea	75	285	2,279
Ericsson (Malaysia) Sdn. Bhd.		Malaysia	70	2	4
Ericsson Telecommunications Pte. Ltd.		Singapore	100	2	1
Ericsson South Africa PTY. Ltd		South Africa	70	—	135
Ericsson Taiwan Ltd.		Taiwan	90	270	36
Ericsson (Thailand) Ltd.		Thailand	49[2]	90	17
Other countries (the rest of the world)			—	—	221
Total					**71,201**
Joint ventures and associated companies					
Concealfab Co		USA	29	7	64
ST-Ericsson SA		Switzerland	50	137	—
Rockstar Consortium Group		Canada	21	1	—
Ericsson Nikola Tesla d.d.		Croatia	49	65	330
Total					**394**

1) Through subsidiary holdings, total holdings amount to 100% of Compania Ericsson S.A.C.I.
2) Through subsidiary holdings, total holdings amount to 100% of Ericsson (Thailand) Ltd.
3) Through subsidiary holdings, total holdings amount to 100% of Ericsson India Private Ltd.

Shares owned by subsidiary companies

Company	Reg. No.	Domicile	Percentage of ownership
Subsidiary companies			
Ericsson Cables Holding AB	556044-9489	Sweden	100
Ericsson France SAS		France	100
Ericsson Telekommunikation GmbH [1]		Germany	100
Ericsson Telecommunicatie B.V.		The Netherlands	100
Ericsson Telekomunikasyon A.S.		Turkey	100
Ericsson Ltd.		United Kingdom	100
Creative Broadcast Services Holdings Ltd.		United Kingdom	100
Ericsson Inc.		United States	100
Ericsson Wifi Inc.		United States	100
Redback Networks Inc.		United States	100
Telcordia Technologies Inc.		United States	83
Ericsson Telecomunicações S.A.		Brazil	100
Ericsson Australia Pty. Ltd.		Australia	100
Ericsson (China) Communications Co. Ltd.		China	100
Nanjing Ericsson Panda Communication Co. Ltd.		China	51
Ericsson Japan K.K.		Japan	100
Ericsson Communication Solutions Pte Ltd.		Singapore	100

Exhibit 6

Excerpts from Nokia Corp.'s Form 20-F Annual Report for Fiscal Year Ended December 31, 2018

Creating the technology to connect the world

As filed with the Securities and Exchange Commission on March 21, 2019

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

FORM 20-F

ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

For the fiscal year ended December 31, 2018

Commission file number 1-13202

Nokia Corporation

(Exact name of Registrant as specified in its charter)

Republic of Finland
(Jurisdiction of incorporation)

Karaportti 3 FI-02610 Espoo, Finland
(Address of principal executive offices)

Esa Niinimäki, Vice President, Corporate Legal, Telephone: +358 (0) 10 44 88 000, Facsimile: +358 (0) 10 44 81 002, Karaportti 3, FI-02610 Espoo, Finland
(Name, Telephone, E-mail and/or Facsimile number and Address of Company Contact Person)

Securities registered pursuant to Section 12(b) of the Securities Exchange Act of 1934 (the "Exchange Act"):

Title of each class	**Name of each exchange on which registered**
American Depositary Shares	New York Stock Exchange
Shares	New York Stock Exchange[1]

(1) Not for trading, but only in connection with the registration of American Depositary Shares representing these shares, pursuant to the requirements of the Securities and Exchange Commission.

Securities registered pursuant to Section 12(g) of the Exchange Act: **None**

Securities for which there is a reporting obligation pursuant to Section 15(d) of the Exchange Act: **None**

Indicate the number of outstanding shares of each of the registrant's classes of capital or common stock as of the close of the period covered by the annual report. Shares: **5 635 945 159**.

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ☒ No ☐

If this report is an annual or transition report, indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or 15(d) of the Exchange Act. Yes ☐ No ☒

Indicate by check mark whether the registrant: (1) has filed all reports required to be filed by Section 13 or 15(d) of the Exchange Act during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T (§232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit such files). Yes ☒ No ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, a smaller reporting company, or an emerging growth company. See the definitions of "large accelerated filer," "accelerated filer", "smaller reporting company" or "emerging growth company" in Rule 12b-2 of the Exchange Act. (Check one):

Large accelerated filer ☒ Accelerated filer ☐
Non-accelerated filer ☐ Smaller reporting company ☐
Emerging growth company ☐

Indicate by check mark which basis of accounting the registrant has used to prepare the financial statements included in this filing:

U.S. GAAP ☐
International Financial Reporting Standards as issued by the International Accounting Standards ☒
Other ☐

If "Other" has been checked in response to the previous question, indicate by check mark which financial statement item the registrant has elected to follow. Item 17 ☐ Item 18 ☐

If this is an annual report, indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ☐ No ☒

Our strategy

Our four pillars

Our strategy builds on our business portfolio and continued drive to create technology that serves people and businesses and includes the following four key priorities.

1 Lead

Lead in high-performance, end-to-end networks with CSPs

Our position

Nokia is a leader in this area today and we will use our main competitive advantage – a near-100% end-to-end portfolio that we can deliver on a global scale – to maintain our leadership while managing for profitability.

Our focus areas

- We are differentiating ourselves with our end-to-end networks that deliver benefits for our customers in automation, total cost of ownership and time to market.
- We are establishing leadership in 5G through our presence with 5G leading customers in the first 5G markets globally and achieving global technology and quality excellence.
- We are innovating in augmented intelligence, analytics and automation for fast and flawless delivery of our network infrastructure services.
- We are providing industry-leading cognitive network services to improve network performance, operational efficiency and subscriber experience, and developing service business models to open new revenue streams for CSPs.
- We are maintaining our leading market share in copper and fiber access, accelerating momentum in fixed wireless access, successfully expanding in the cable market, further developing new smart home solutions such as whole-home Wi-Fi, and simplifying network operations for our customers.
- We are leveraging our superior products and the next-generation IP routing portfolio based on our FP4 chipset to grow in both edge and core routing, where we have a fully virtualized portfolio that is differentiated by performance, flexibility, security and quality.

Progress

- We are driving the deployment of 5G: the number of customers already engaged with us on 5G is rapidly heading over the 100 mark, and amongst those we have already signed over 25 5G supply agreements. Our global base of mobile broadband customers puts us in a position of strength as 5G rollouts accelerate globally.
- In July, 2018, we announced a landmark USD 3.5 billion agreement with T-Mobile to accelerate the deployment of their nationwide 5G network in the United States. During the year we also signed three separate framework agreements with a combined value of EUR 2 billion with China Mobile, China Telecom and China Unicom.
- Independent third party assessments by P3/Connect and others testify to Nokia's superior networks performance around the world.

2 Expand

Expand network sales to select vertical markets

Our position

We continue to expand into select vertical markets that have high-performance, carrier-grade networking needs: Web and cloud companies; transportation, energy, public sector (TEPS); and TXLE (large enterprises for which technology is a strategic advantage). As the world becomes more digital and more automated, the kind of high-performance, low-latency networks once used almost exclusively in telecommunications are now needed by other organizations. This is especially true in organizations that own high-value, movable assets that are mission-critical. To address this growing need for high-performance networks, Nokia formed the Nokia Enterprise business group. With Nokia Enterprise, we have implemented a combined sales organization, a targeted portfolio and new solutions that address our customers' digitization and automation needs.

Our focus areas

- Web and cloud customers increasingly require high-performance networks to improve customer experiences and to expand their primary business models. For web and cloud companies, we are focusing on an all-IP-led approach, providing IP routing and optical network infrastructure.
- Large, tech-savvy enterprise (TXLE) customers need to virtualize and automate their hybrid cloud data centers with technology disruptions like software-defined wide area networking (SD-WAN), software-defined security, and branch office connectivity. Nokia can address those needs with SD-WAN and our all-IP portfolio.
- TEPS customers require high-performance, mission-critical networking that digitizes their energy systems, rail systems and cities. They also need to layer on top of those networks industrial automation platforms that help digitize their operations. Nokia offers mission-critical networks, solutions for digitization and Industrial IoT, and industrial automation.
- Other verticals also need to increase productivity and reduce costs through the digitization and automation of their operational systems. This can be accomplished with Industrial IoT platforms, automation platforms and private wireless networks. Nokia now targets these opportunities.

Progress

- In 2018 we made good progress in our select vertical markets with over 150 new customers and we now have more than 1 000 enterprise customers. We consolidated our enterprise-specific activities into Nokia Enterprise, our new business group, which commenced operations January 1, 2019.
- In 2018 we delivered constant currency sales growth of 9% in the enterprise space, excluding the third-party business that we are exiting, and posted solid profitability.
- We unveiled our "Future X for industries" strategy and architecture, which leverages digital transformation technologies to catalyze productivity and economic growth for enterprises.
- We also announced numerous private LTE deals during the year including Elektro, a power distributor in Brazil, and BMW's smart manufacturing facility in partnership with China Unicom.

32. Principal Group companies

The Group's significant subsidiaries as of December 31, 2018:

Company name	Country of incorporation	Parent holding %	Group ownership interest %
Nokia Solutions and Networks B.V.	Netherlands	–	100.0
Nokia Solutions and Networks Oy	Finland	100.0	100.0
Nokia of America Corporation	USA	–	100.0
Nokia Solutions and Networks India Private Limited	India	–	100.0
Nokia Technologies Oy	Finland	100.0	100.0
Alcatel-Lucent Participations SA	France	–	100.0
Nokia Canada Inc.	Canada	–	100.0
Nokia Shanghai Bell Co., Ltd[1]	China	–	50.0
Nokia Solutions and Networks Branch Operations Oy	Finland	–	100.0
Nokia Solutions and Networks Japan G.K.	Japan	–	100.0
Alcatel Submarine Networks SAS	France	–	100.0
Nokia Spain, S.A.	Spain	–	100.0
Alcatel-Lucent Italia S.p.A.[2]	Italy	–	100.0
Alcatel Lucent SAS	France	–	100.0
Nokia UK Limited	UK	–	100.0
Nokia Solutions and Networks GmbH & Co. KG	Germany	–	100.0
Alcatel-Lucent International SA	France	–	100.0
Nokia Services Limited	Australia	–	100.0
PT Nokia Solutions and Networks Indonesia	Indonesia	–	100.0
Alcatel-Lucent Brasil Telecomunicações Ltda	Brazil	–	100.0
Nokia Solutions and Networks do Brasil Telecomunicações Ltda.	Brazil	–	100.0

(1) Nokia Shanghai Bell Co., Ltd is the parent company of the Nokia Shanghai Bell joint venture of which the Group owns 50% plus one share with China Huaxin, an entity controlled by the Chinese government, holding the remaining ownership interests. Refer to Note 33, Significant partly-owned subsidiaries.
(2) Alcatel-Lucent Italia S.p.A. merged into Nokia Solutions and Networks Italia S.p.A., effective January 1, 2019.

33. Significant partly-owned subsidiaries

As part of the acquisition of Alcatel Lucent on January 4, 2016, the Group acquired a partly-owned consolidated subsidiary, Alcatel-Lucent Shanghai Bell Co., Ltd. On May 18, 2017, the Group announced the signing of definitive agreements with the China Huaxin Post & Telecommunication Economy Development Center (China Huaxin) related to the integration of Alcatel-Lucent Shanghai Bell Co,. Ltd. and the Group's China business into a new joint venture branded as Nokia Shanghai Bell.

As part of the definitive agreements, the Group transferred it's China business and subsidiaries to Nokia Shanghai Bell in exchange for a cash payment. As the transfer of the Group's China business consisted of a transaction between two Group subsidiaries, all gains or losses that arose from the transaction were fully eliminated within the Group's consolidated financial statements. Further, the transfer of cash from Nokia Shanghai Bell to the wholly-owned parent entity of the Group's China business did not impact the cash nor net cash balances in the Group's consolidated financial statements.

On July 3, 2017, the Group and China Huaxin commenced operations of the new Nokia Shanghai Bell joint venture. The Group holds an ownership interest of 50% plus one share in the Nokia Shanghai Bell's parent company, Nokia Shanghai Bell Co., Ltd., with China Huaxin holding the remaining ownership interests. The definitive agreements provide China Huaxin with the right to fully transfer its ownership interest in Nokia Shanghai Bell to the Group and the Group with the right to purchase China Huaxin's ownership interest in Nokia Shanghai Bell in exchange for a future cash settlement. As a result, the Group derecognized the non-controlling interest balance related to Nokia Shanghai Bell of EUR 772 million partly offset by the recognition of a related financial liability of EUR 737 million with the difference of EUR 35 million recorded as a gain within retained earnings as a transaction with the non-controlling interest.

The financial liability is measured based on the present value of the expected future cash settlement to acquire the non-controlling interest in Nokia Shanghai Bell. In 2018, the net present value of the expected future cash settlement amounted to EUR 693 million (EUR 672 million in 2017) and an interest expense of EUR 39 million (EUR 18 million in 2017) was recorded to reflect the recognition of the present value discount on the financial liability. In addition, the Group decreased the value of the financial liability to reflect a change in estimate of the future cash settlement resulting in the recognition of a EUR 6 million gain (EUR 64 million in 2017) in financial income and expenses in the consolidated income statement. In 2018, the Group reclassified the financial liability from non-current liabilities to current liabilities which is in line with the option exercise period.

Financial information for the Nokia Shanghai Bell Group[1]:

EURm	2018	2017
Summarized income statement		
Net sales[2]	2 518	2 276
Operating profit	54	83
Profit for the year	25	52
Profit for the year attributable to:		
Equity holders of the parent	25	15
Non-controlling interests[3]	–	37
Summarized statement of financial position		
Non-current assets	600	589
Non-current liabilities	(127)	(130)
Non-current net assets	**473**	**459**
Current assets[4]	3 340	3 888
Current liabilities	(2 209)	(2 765)
Current net assets	**1 131**	**1 123**
Net assets[5]	**1 604**	**1 582**
Non-controlling interests[6]	–	–
Summarized statement of cash flows		
Net (used in)/from operating activities	(103)	438
Net cash used in investing activities	(92)	(184)
Net cash used in financing activities	(63)	(442)
Net decrease in cash and cash equivalents	**(258)**	**(188)**

(1) Financial information for the Nokia Shanghai Bell Group is presented before eliminations of intercompany transactions with the rest of the Group but after eliminations of intercompany transactions between entities within the Nokia Shanghai Bell Group.
(2) Includes EUR 268 million (EUR 328 million in 2017) net sales to other Group entities.
(3) In 2017, profit for the year is attributed to non-controlling interests until July 3, 2017.
(4) Includes a total of EUR 738 million (EUR 1 001 million in 2017) of cash and cash equivalents and current financial investments.
(5) The distribution of the profits of Nokia Shanghai Bell Co., Ltd requires the passing of a special resolution by more than two-thirds of its shareholders, subject to a requirement that at least 50% of the after-tax distributable profits are distributed as dividends each year.
(6) In 2017, the non-controlling interest balance was derecognized and partially offset by the recognition of the related financial liability of EUR 737 million.

Exhibit 7

Excerpts from Nokia Corp.'s Form 20-F Annual Report for Fiscal Year 2017

Creating the technology to connect the world

As filed with the Securities and Exchange Commission on March 22, 2018

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

FORM 20-F

ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

For the fiscal year ended December 31, 2017

Commission file number 1-13202

Nokia Corporation

(Exact name of Registrant as specified in its charter)

Republic of Finland
(Jurisdiction of incorporation)

Karaportti 3 FI-02610 Espoo, Finland
(Address of principal executive offices)

Jussi Koskinen, Vice President, Corporate Legal, Telephone: +358 (0) 10 44 88 000, Facsimile: +358 (0) 10 44 81 002, Karaportti 3, FI-02610 Espoo, Finland
(Name, Telephone, E-mail and/or Facsimile number and Address of Company Contact Person)

Securities registered pursuant to Section 12(b) of the Securities Exchange Act of 1934 (the "Exchange Act"):

Title of each class	**Name of each exchange on which registered**
American Depositary Shares	New York Stock Exchange
Shares	New York Stock Exchange[1]

(1) Not for trading, but only in connection with the registration of American Depositary Shares representing these shares, pursuant to the requirements of the Securities and Exchange Commission.

Securities registered pursuant to Section 12(g) of the Exchange Act: **None**

Securities for which there is a reporting obligation pursuant to Section 15(d) of the Exchange Act:
5.375% Notes due 2019, 3.375% Notes due 2022, 4.375% Notes due 2027 and 6.625% Notes due 2039.

Indicate the number of outstanding shares of each of the registrant's classes of capital or common stock as of the close of the period covered by the annual report. Shares: **5 839 404 303**.

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ☒ No ☐

If this report is an annual or transition report, indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or 15(d) of the Exchange Act. Yes ☐ No ☒

Indicate by check mark whether the registrant: (1) has filed all reports required to be filed by Section 13 or 15(d) of the Exchange Act during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically and posted on its corporate Web site, if any, every Interactive Data File required to be submitted and posted pursuant to Rule 405 of Regulation S-T (§232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit and post such files). Yes ☒ No ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, or a smaller reporting company. See the definitions of "large accelerated filer," "accelerated filer" and "smaller reporting company" in Rule 12b-2 of the Exchange Act. (Check one):

Large accelerated filer ☒ Accelerated filer ☐
Non-accelerated filer ☐ (Do not check if a smaller reporting company) Smaller reporting company ☐

Indicate by check mark which basis of accounting the registrant has used to prepare the financial statements included in this filing:

U.S. GAAP ☐
International Financial Reporting Standards as issued by the International Accounting Standards Board ☒
Other ☐

If "Other" has been checked in response to the previous question, indicate by check mark which financial statement item the registrant has elected to follow. Item 17 ☐ Item 18 ☐

If this is an annual report, indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ☐ No ☒

Within our Networks business

Sales and marketing

The Customer Operations ("CO") organization is responsible for sales and account management across the five network-oriented business groups. The CO teams are represented worldwide (in approximately 130 countries) to ensure that we are close to our customers and have a deep understanding of local markets. In this way, we strive to create and maintain deep customer intimacy across our customer base.

Geographically, the CO organization is divided into seven markets:

- **Asia-Pacific and Japan** spans a varied geographical scope, ranging from advanced telecommunications markets, such as Japan and the Republic of South Korea, to developing markets including Philippines, Bangladesh, Myanmar, Vietnam and others. In 2017, we worked with all the leading operators in the market, and collaborated on 5G, IoT and other leading network evolution topics with operators from Japan and the Republic of South Korea. We also run a major Service Delivery Hub in Japan. Furthermore, we work across a wide range of vertical markets in Asia-Pacific and Japan including public sector, transportation and energy enabling solutions through its end-to-end portfolio.
- In **Europe**, we engaged with all the major operators serving millions of customers. We have extensive R&D expertise in Europe, and some of our largest Technology Centers, which are developing future technologies, are based in this market. We also have a Global Delivery Center (across two locations: Portugal and Romania) and three regional Service Delivery Hubs in Europe (one in Russia and two in Poland). With our strong end-to-end portfolio, Nokia is well positioned in Europe to help maximize the benefits of 5G, IoT and the digital transformation in the local digital ecosystems.
- In **Greater China**, we are the leading player among companies headquartered outside China, and work with all the major operators. We have also extended our market presence to the public and enterprise sectors, including energy, railways and public security. In 2017, we worked with numerous China-based webscale companies, and all the major operators in Taiwan. In China, we have six Technology Centers, one regional Service Delivery Hub and more than 80 offices spread over megacities and provinces. A major achievement in 2017 was the closing of our agreement with our Chinese partner, which resulted in the formation of the joint venture—Nokia Shanghai Bell. This was the last major organizational step in Nokia and Alcatel Lucent integration, bringing together approximately 8 000 colleagues from both companies into a single organization.
- In **India**, we are a strong supplier and service provider to the leading public and private operators. Collectively, our networks for these operators serve 418 million subscribers across some 459 000 sites with Nokia managing networks supporting 154 million subscribers. In addition, we are a key telecom infrastructure supplier to non-operator segments, including large enterprises, utilities companies, and the Indian defense sector. We are also a strategic telecommunications partner in GSM-Railways technology in India. Nokia's operations in the country include a Global Delivery Center, a Service Delivery Hub and a Global Technology Center.
- In **Latin America**, an estimated 24% of mobile subscribers use LTE services, almost double from a year ago, due to accelerated adoption in Brazil, Mexico and Argentina. High-speed fixed broadband, meanwhile, is still in its early phase. With the aim of providing broadband services to a population of over 600 million people in the area, we supplied ultra-competitive solutions to all major operators. In 2017, we also closed our biggest ever deal in the market—the nationwide wholesale LTE network in Mexico known as 'Red Compartida', for Altán Redes, and the largest LTE 700 MHz deployment in Brazil with TIM.
- In **Middle-East and Africa**, we see strong opportunities for Nokia, and we are closely working with all key global and regional operators. We have been laying the foundation for early 5G adoption and Smart Cities deployments in the Middle-East region, and continue to see strong growth in the number of mobile broadband users in Africa, driven by increasing affordability of smartphones and commercial LTE deployments across the continent.
- In **North America**, we count all the major operators as our key customers. We also deliver advanced IP networking, ultra-broadband access, and cloud technology solutions to a wide array of customers, including local service providers, cable operators, large enterprises, state and local governments, utilities, and many others. North America is also home to the our most important and thriving innovation practices—from the renowned Nokia Bell Labs headquarters in Murray Hill, New Jersey, to the development labs in Silicon Valley.

Exhibit 8

Excerpts from China Mobile Ltd.'s Form 20-F Annual Report for Fiscal Year 2018

Table of Contents

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, DC 20549

FORM 20-F

☐ **REGISTRATION STATEMENT PURSUANT TO SECTION 12(b) OR 12(g) OF THE SECURITIES EXCHANGE ACT OF 1934**

OR

☒ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the fiscal year ended December 31, 2015

OR

☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the transition period from _____ to _____

OR

☐ **SHELL COMPANY REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

Date of event requiring this shell company report _____

Commission file number: 1-14696

China Mobile Limited
(Exact Name of Registrant as Specified in Its Charter)

N/A
(Translation of Registrant's Name into English)

Hong Kong, China
(Jurisdiction of Incorporation or Organization)

60th Floor, The Center
99 Queen's Road Central
Hong Kong, China
(Address of Principal Executive Offices)

Grace Wong
Company Secretary
China Mobile Limited
60th Floor, The Center
99 Queen's Road Central
Hong Kong, China
Telephone: (852) 3121-8888
Fax: (852) 2511-9092
(Name, Telephone, E-mail and/or Facsimile Number and Address of Company Contact Person)

Securities registered pursuant to Section 12(b) of the Act:

Title of Each Class	Name of Each Exchange on Which Registered
Ordinary shares	**New York Stock Exchange***

*** Not for trading, but only in connection with the listing on the New York Stock Exchange of American depositary shares representing the ordinary shares.**

Securities registered or to be registered pursuant to Section 12(g) of the Act:

None
(Title of Class)

Securities for which there is a reporting obligation pursuant to Section 15(d) of the Act:

None
(Title of Class)

Indicate the number of outstanding shares of each of the issuer's classes of capital or common stock as of the close of the period covered by the annual report.

As of December 31, 2015, 20,475,482,897 ordinary shares were issued and outstanding.

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ☒ No ☐

If this report is an annual or transition report, indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or (15)(d) of the Securities Exchange Act of 1934. Yes ☐ No ☒

Note — Checking the box above will not relieve any registrant required to file reports pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 from their obligations under those Sections.

Indicate by check mark whether the registrant: (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically and posted on its corporate Web site, if any, every Interactive Data File required to be submitted and posted pursuant to Rule 405 of Regulation S-T during the preceding 12 months (or for such shorter period that the registrant was required to submit and post such files). Yes ☐ No ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, or a non-accelerated filer. See definition of "accelerated filer and large accelerated filer" in Rule 12b-2 of the Exchange Act. (Check one):

Large accelerated filer ☒	Accelerated filer ☐	Non-accelerated filer ☐

Indicate by check mark which basis of accounting the registrant has used to prepare the financial statements included in this filing.

U.S. GAAP ☐	International Financial Reporting Standards as issued by the International Accounting Standards Board ☒	Other ☐

If "Other" has been checked in response to the previous question, indicate by check mark which financial statement item the registrant has elected to follow. Item 17 ☐ Item 18 ☐

If this is an annual report, indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ☐ No ☒

Under our Articles of Association, our directors and senior management do not have different voting rights when compared to other holders of shares in the same class.

As of December 31, 2015, there were no outstanding options exercisable to subscribe for shares in our Company granted to our directors and members of our senior management under our share option scheme.

Item 7. Major Shareholders and Related Party Transactions.

Major Shareholders

As of March 31, 2016, approximately 72.72% of our outstanding shares were held by China Mobile Hong Kong (BVI) Limited, a wholly-owned subsidiary of China Mobile (Hong Kong) Group Limited. CMCC, a state-owned company, holds all of the voting shares and economic interest in China Mobile (Hong Kong) Group Limited. No other persons own 5% or more of our ordinary shares. Between our initial public offering and March 31, 2016, our majority shareholders held, directly or indirectly, between approximately 72.72% and 76.5% of equity interest in us, except for brief periods following our equity offerings in 1999 and 2000 but before the issuance of consideration shares to our direct shareholder, China Mobile Hong Kong (BVI) Limited, for the related acquisitions, during which periods the shareholding was temporarily lower. See "Item 4. Information on the Company — The History and Development of the Company — Industry Restructuring and Changes in Our Shareholding Structure" for changes during the past three years with respect to our majority shareholders. Under our Articles of Association, our major shareholders do not have different voting rights when compared to other holders of shares in the same class.

We are not aware of any arrangement which may at a subsequent date result in a change of control over us.

Related Party Transactions

As of March 31, 2016, CMCC indirectly owned an aggregate of approximately 72.72% of our issued and outstanding share capital.

We and each of our subsidiaries have entered into various related party transactions. The principal terms of the agreements for these related party transactions are described below.

Certain charges for the services under these agreements are based on tariffs set by the PRC regulatory authorities. Those transactions where the charges are not set by PRC regulatory authorities are based on commercial negotiation between the parties, in each case on an arm's-length basis.

International Roaming Arrangements

Pursuant to an agreement between us and CMCC (the "International Roaming Settlement Agreement"), CMCC maintains the existing settlement arrangements with respect to international interconnection and roaming with the relevant telecommunications services providers in foreign countries and regions, and collects the relevant usage fees and other fees from us and pays the same to the relevant mobile services providers in foreign countries and regions. On September 13, 2012, we entered into an agreement with CMCC, pursuant to which CMCC would gradually transfer its settlement arrangements with certain telecommunications services providers in foreign countries and regions to China Mobile International, our wholly-owned subsidiary. As a result, our arrangement with CMCC with respect to international interconnection and roaming with those telecommunications services providers has been gradually phasing out.

Licensing of Trademark

CMCC is the owner of the "CHINA MOBILE" name and logo, a registered trademark in Mainland China, Australia, Brunei, Cambodia, Canada, Hong Kong, India, Indonesia, Macau, New Zealand, Pakistan, South Africa, South Korea, Taiwan, Thailand, the United States and Yemen. In addition, it has filed applications to register the "CHINA MOBILE" name and logo as a trademark in Malaysia for certain goods and services. CMCC has also registered the "CHINA MOBILE" name and logo as a trademark under the Protocol Relating to the Madrid Agreement Concerning the International Registration of Marks.

Exhibit 9

"FCC Denies China Mobile's Bid to Provide International Telecom Services in the U.S."

BUSINESS

FCC Denies China Mobile's Bid to Provide International Telecom Services in the U.S.

Regulators cited a review that determined Chinese state ownership of the company posed national security and law enforcement risks

A staffer for the Federal Communications Commission said Thursday that China Mobile is "subject to exploitation, influence and control by the Chinese government." PHOTO: SERGIO PEREZ/REUTERS

By Ryan Tracy

Updated May 9, 2019 1:33 p.m. ET

WASHINGTON—The U.S. blocked a Chinese telecom giant from providing services via American networks, the latest sign of escalating tension between the two global powers.

The Federal Communications Commission voted unanimously to deny an application by China Mobile Ltd.'s U.S. arm, China Mobile USA, to provide international calls and other services. U.S. officials cited law enforcement and national security risks, saying the company is owned by the Chinese government and vulnerable to exploitation, influence and control.

"The Chinese government could use China Mobile to exploit our telephone network to increase intelligence collection against U.S. government agencies and other sensitive targets that depend on this network," FCC Chairman Ajit Pai said. "That is a flatly unacceptable risk."

The FCC's denial comes at a sensitive time, with the two countries in the final stages of negotiating a difficult trade deal and financial markets on edge over the prospect of a deteriorating China-U.S. relationship. China Mobile is by some measures the world's largest

mobile telecommunications firm. The parent company didn't immediately respond to an email requesting comment Thursday.

In a May 1 letter to the commission, an attorney representing China Mobile said it "continues to believe that this action is guided more by tensions in the bilateral U.S.-China relationship than an absence of" options to mitigate regulators' concerns.

The FCC's 5-0 vote underscored bipartisan concern about the application, originally filed in 2011. The expected move came after a yearslong review by U.S. agencies recommended in July 2018 that the FCC deny China Mobile's request.

It was the first time the U.S. government has recommended denying an application to provide telecom services based on national security and law enforcement concerns, the FCC said. The agencies determined China Mobile USA "would likely comply with espionage and intelligence requests made by the Chinese government," according to the FCC.

The FCC could go further. Mr. Pai said the agency is reviewing whether two other Chinese telecom firms, operating in the U.S., should retain permits.

"Security threats have evolved over the many years since those companies were granted interconnection rights to U.S. networks in the early 2000s," said FCC Commissioner Brendan Carr said.

The decision was the latest of the Trump administration's efforts to block Chinese firms from gaining control of U.S. companies in technology and other sectors. Earlier this year, the U.S. ordered Beijing Kunlun Tech Co. Ltd to sell its majority stake in the dating app Grindr, citing the risk that the personal data collected via the app could be use to blackmail individuals with U.S. security clearances, The Wall Street Journal reported in March.

Last year, U.S. regulators blocked the sale of the Chicago stock exchange to a group that would have included Chinese investors.

China Mobile is considered a state-owned enterprise, but also is listed on the New York Stock Exchange and in Hong Kong.

Write to Ryan Tracy at ryan.tracy@wsj.com

Exhibit 10

"Company Overview" of China Telecom (Americas)

CHINA TELECOM AMERICAS

Company Overview

Headquartered in Herndon, Virginia, China Telecom Americas is the largest international subsidiary of China Telecom Corporation Limited, as well as the only authorized re-seller of domestic Chinese telecom products to North American companies. China Telecom Americas has offices in 31 countries, providing access to Chinese telecom network assets for customers in the United States, Canada and Latin America.

As the largest operating broadband operator in the world (127 million subscribers), as well as the world's largest CDMA mobile operator (227 million subscribers), China Telecom delivers a comprehensive global telecom service scope based on cutting edge technology, exceptional customer service, and a visionary approach to international telecommunications.

China Telecom's core strengths in facts & figures:

- World's largest fixed line operator (144 million fixed access lines in service).
- World's largest broadband operator (127 million subscribers)
- World's largest CDMA mobile operator (227 million subscribers, including 147 million 4G subscribers)
- Owns and operates China's largest optical fiber network: over 83,000 km long, covering 70% of China's territory and connecting all Chinese cities
- Owns and operates ChinaNet, China's largest Internet network
- Owns and operates China's largest MPLS VPN network, based on CN2, our next-generation, carrier-class, IPv6-capable Internet backbone network
- Primary service provider in all 21 southern provinces in China.
- Owns comprehensive trans-Pacific cable systems, including China-U.S., Japan-U.S., SEA-ME-WE3 in APCN2, SMW3, SMW5, FASTER, Flag, TAE, etc.
- International bilateral connectivity to 100+ countries
- More than 670,000 professionals employed around the world

- Ranked #132 on Fortune's Global 500 in 2016.

Latest News

- China Telecom, Tata Communications Partner to drive global connectivity for IoT devices
- China Telecom Backs Launch of GSMA's Digital Declaration at Davos
- Sharktech Adds China Telecom CN2 to Los Angeles Network Offering
- Keysight Technologies, China Telecom Collaborate To Accelerate Commercial Deployment Of 5G Technology
- Breakthrough for "the Belt and Road Initiative" project, China Telecom completes the first direct access optical fibe...

MORE NEWS

Insights

- China Telecom Implements a Low Voltage System for Minghua's $45 million Spartanburg plant
- China Telecom, Shenzhen Water Group Deliver the World's First Commercial NB-IoT-based Water Management Platform
- China Telecom Showcases Smart Waste Management Platform at the 2017 World Internet Conference in Wuzhen, China
- The Benefits of SD-WAN for a Globalized IT Economy
- China Data Center Trends and Future Outlook

MORE INSIGHTS

Events

- JUNE 9 - 13, 2019**Cisco Live**San Diego, CA | Booth 3532
- APRIL 9 - 12, 2019**Channel Partners**Las Vegas, NV | Booth 344
- APRIL 9 - 11, 2019**Google Cloud Next '19**San Francisco, CA
- APRIL 8 - 9, 2019**WAN Summit 2019**New York, NY | Table Number 6
- MARCH 10-13, 2019**Super9 Convergence**Nashville, TN | Table #24

https://www.ctamericas.com/company/company-overview/

MORE EVENTS

Contact Us

Questions about which solutions are right for your organization? We can help!

Exhibit 11

Excerpts from China Telecom Corp. Ltd.'s Form 20-F Annual Report for Fiscal Year 2018

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, DC 20549

FORM 20-F

☐ **REGISTRATION STATEMENT PURSUANT TO SECTION 12(b) OR 12(g) OF THE SECURITIES EXCHANGE ACT OF 1934**

OR

☒ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the fiscal year ended December 31, 2018

OR

☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

OR

☐ **SHELL COMPANY REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

Date of event requiring this shell company report

For the transition period from to

Commission file number 1-31517

中国电信股份有限公司
(Exact Name of Registrant as Specified in Its Charter)

China Telecom Corporation Limited

(Translation of Registrant's Name into English)

People's Republic of China
(Jurisdiction of Incorporation or Organization)

31 Jinrong Street, Xicheng District
Beijing, People's Republic of China 100033
(Address of Principal Executive Offices)

Ms. Wong Yuk Har, Rebecca
China Telecom Corporation Limited
28/F, Everbright Centre
108 Gloucester Road
Wanchai, Hong Kong
Email: rebecca.wong@chinatelecom-h.com
Telephone: (+852) 2582 5819
Fax: (+852) 2157 0010
(Name, Telephone, E-mail and/or Facsimile number and Address of Company Contact Person)

Securities registered or to be registered pursuant to Section 12(b) of the Act:

Title of Each Class	Name of Each Exchange On Which Registered
American depositary shares	**New York Stock Exchange, Inc.**
H shares, par value RMB1.00 per share	**New York Stock Exchange, Inc.***

* Not for trading, but only in connection with the listing on the New York Stock Exchange, Inc. of American depositary shares, each representing 100 H shares.

Securities registered or to be registered pursuant to Section 12(g) of the Act:

None
(Title of Class)

Securities for which there is a reporting obligation pursuant to Section 15(d) of the Act:

None
(Title of Class)

Indicate the number of outstanding shares of each of the issuer's classes of capital or common stock as of the close of the period covered by the annual report.

As of December 31, 2018, 67,054,958,321 domestic shares and 13,877,410,000 H shares, par value RMB1.00 per share, were issued and outstanding. H shares are ordinary shares of the Company listed on The Stock Exchange of Hong Kong Limited.

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ☒ No ☐

If this report is an annual or transition report, indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934. Yes ☐ No ☒

Indicate by check mark whether the registrant: (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T (§232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit such files) Yes ☒ No ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, or an emerging growth company. See definition of "large accelerated filer," "accelerated filer," and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large Accelerated Filer ☒ Accelerated Filer ☐ Non-Accelerated Filer ☐ Emerging Growth Company ☐

If an emerging growth company that prepares its financial statements in accordance with U.S. GAAP, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards† provided pursuant to Section 13 (a) of the Exchange Act. ☐

† The term "new or revised financial accounting standard" refers to any update issued by the Financial Accounting Standards Board to its Accounting Standards Codification After April 5, 2012.

Indicate by check mark which basis of accounting the registrant has used to prepare the financial statements included in this filing.

U.S. GAAP ☐

International Financial Reporting Standards as issued by the International Accounting Standards Board ☒

Other ☐

If "Other" has been checked in response to the previous question, indicate by check mark which financial statement item the registrant has elected to follow. Item 17 ☐ Item 18 ☐

If this is an annual report, indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ☐ No ☒

(APPLICABLE ONLY TO ISSUERS INVOLVED IN BANKRUPTCY PROCEEDINGS DURING THE PAST FIVE YEARS)

Indicate by check mark whether the registrant has filed all documents and reports required to be filed by Sections 12, 13 or 15(d) of the Securities Exchange Act of 1934 subsequent to the distribution of securities under a plan confirmed by a court. Yes ☐ No ☐

We cannot assure you that we can obtain sufficient financing at commercially reasonable terms or at all. If adequate capital is not available on commercially reasonable terms, our growth potential and prospects could be materially and adversely affected. Furthermore, additional issuances of equity securities will result in dilution to our shareholders. Incurrence of debt would result in increased interest expense and could require us to agree to restrictive operating and financial covenants.

If we are not able to respond successfully and cost-efficiently to technological or industry developments, our business may be materially and adversely affected.

The telecommunications market is characterized by rapid advancements in technology, evolving industry standards and changes in customer needs. We cannot assure you that we will be successful in responding to these developments. In addition, new services or technologies, such as mobile Internet, the three-network convergence, cloud computing and Internet of Things, may render our existing services or technologies less competitive. In the event we do take measures to respond to technological developments and changes in industry standards, the integration of new technology or industry standards or the upgrading of our networks may require substantial time, effort and capital investment. Moreover, the successful deployment and application of such cutting edge technologies depend on a number of factors, including the integration of legacy networks and cloud security related challenges. We cannot assure you that we will succeed in integrating these new technologies and industry standards or adapting our network and systems in a timely and cost-effective manner, or at all. Our inability to respond successfully and cost-efficiently to technological or industry developments may materially and adversely affect our business, results of operations and competitiveness.

Our ability to respond to technological developments in a cost-efficient manner may also be adversely affected by external factors, some of which are beyond our control. For example, the development in 5G technology is expected to have a major impact on our services. We have been engaged in standards formulation, network technology trial runs as well as planning of the application of 5G services towards commercialization. In December 2018, China Telecom Group was granted the approval from the MIIT to utilize the 3400-3500MHz spectrum nationwide for 5G system trial until June 30, 2020. In addition, we have been taking the initiatives to explore the feasibility of collaborative development of 5G and 4G. We have devoted, and will continue to devote, substantial resources in the development of 5G technology. However, various details concerning 5G services are still uncertain, including the timing of the issuance of 5G permits, the frequency bands allocated to 5G services and relevant regulations. In addition, there is no assurance that we will be able to roll out 5G services in an economically viable manner to gain favorable market share based on reasonable commercial terms with business partners without undue delay. Furthermore, the 5G industry chain is still under development, and we continue to explore 5G services' business model and commercial applications. If we are unable to respond to these uncertainties, the expected benefits from our investment in development of 5G technology would not be fully realized or at all and such inability to respond to these uncertainties may materially and adversely affect our business in the future.

We are subject to risks associated with our telecommunications equipment suppliers and other business partners which could be adversely affected by restrictions, sanctions or other legal or regulatory actions under relevant laws and regulations in various jurisdictions which in turn could adversely affect the supply chain and our business operations.

We procure our telecommunications network equipment and related maintenance and technical support from certain PRC and overseas telecommunications equipment suppliers. See "Item 4. Information on the Company—B. Business Overview—Network System". We also transact business with our business partners who may operate globally. As these parties operate globally and are therefore subject to the laws and regulations in various jurisdictions, any restrictions, sanctions or other legal or regulatory actions could cause disruptions or other material difficulties in their business activities to the extent any government of the relevant jurisdictions imposes any restrictions on their import and export activities, or sanctions or other legal or regulatory actions against the suppliers and other business partners in connection with their business activities. The relevant jurisdictions include, among others, the United States, the European Union and the United Nations. Furthermore, as the supply of our telecommunications equipment relies on a global supply chain, which is vulnerable to significant disruptions in the supply of parts and other items that are necessary for the relevant manufacturing activities. Such disruptions could prevent those affected suppliers from delivering equipment and services to us in accordance with the agreed terms of supply, which in turn could negatively affect our business operations. For example, we may not be able to find suitable alternative suppliers for the affected equipment in a timely manner. Even if we are able to find alternative suppliers, the commercial terms may not be comparable, and we could therefore be subject to a higher procuring cost. Furthermore, if any of our suppliers raises their prices due to an increase in international trade tariffs, we could be subject to a higher cost in procuring the relevant products. We may experience a significant delay in implementing the part of our business plans that relies on delivery of the affected network equipment and difficulties in timely improving our services that rely on those suppliers for upgrading our networks and related software and applications. Any of these and other consequences could materially adversely affect our business, results of operations, financial condition and prospect and cause a significant volatility in and a decline in our share price.

Universal Services

Under the Telecommunications Regulations, telecommunications service providers in the PRC are required to fulfill universal service obligations in accordance with relevant regulations promulgated by the PRC government, and the MIIT has been given authority by the PRC government to delineate the scope of its universal service obligations. The MIIT, together with other regulatory authorities, is also responsible for formulating administrative rules relating to the establishment of a universal service fund and compensation schemes for universal services. The State Council issued the Notice on the "Broadband China" Policy and the Implementation Plan on August 1, 2013, which included the provision of broadband services to remote villages as part of the universal service obligations of telecommunications service providers and mentioned improving the compensation scheme for the expenses incurred in the "Broadband China" projects undertaken by telecommunications service providers in the villages. In addition, the MOF and the MIIT jointly issued the Notice of Implementation of Telecommunications Universal Services Pilot Work in December 2015, which provided that the telecommunications universal services should take a market-oriented approach and that the telecommunications universal services providers should be selected through a public bidding process. This notice sets up certain goals for the telecommunications operators, including broadband coverage in 98% of the administrative villages and over 12Mbps broadband access capacity in rural villages, by 2020. Pursuant to the notice, the central government subsidies will be granted to the pilot areas determined by the MOF and the MIIT and the universal services providers will be selected through an open bidding process.

The PRC government used financial resources to compensate the expenses incurred in the "Coverage to All Villages" and the "Broadband China" projects before the implementation of universal services pilot projects in 2016. We, together with other telecommunications operators, have undertaken the "Coverage to All Villages" project since 2004. Since 2016, we have undertaken universal services pilot projects in accordance with the requirements of the Chinese government and in aggregate won the bids to undertake the construction of broadband network facilities in approximately 50,000 administrative villages in 19 provinces and autonomous regions. By the end of 2018, we had completed the construction of broadband networks in approximately 50,000 administrative villages. Since 2018, the PRC government included 4G network coverage into the scope of pilot projects for universal services. We have continuously promoted the construction of communication networks in rural areas and remote rural villages and strives to improve the broadband access coverage in rural areas. In addition, we have set up local service points for rural villages, actively promoted the development of e-commerce in rural areas, and strived to contribute to the informatization upgrade and revitalization of rural areas in various regions. The compensation from the PRC government may not be sufficient to cover all of our expenses for providing the telecommunications universal services. However, we believe the expenses for such operation and maintenance will not have a material effect on our financial condition.

State-Owned Assets Supervision

Under the PRC Company Law, PRC Enterprise State-Owned Assets Law, Interim Measures for the Supervision and Administration of State-Owned Assets of the Enterprises, and other administrative regulations, the SASAC, among others, supervises the preservation of the value of state-owned assets, guides the reform and restructuring of state-owned enterprises, and evaluates the performance of management executives of state-owned enterprises through legal procedures. Our controlling shareholder, China Telecom Group, is a state-owned enterprise owned by the SASAC and subject to the SASAC's supervision.

As part of the PRC government's efforts to reform state-owned enterprises and increase their competitiveness, the PRC government has selected certain enterprises of designated industries, including the telecommunications industry, as the first group of state-owned enterprises for a pilot program on state-owned enterprise mixed ownership reform. Unicom Group was selected among the operators of the telecommunications industry to join such mixed ownership reform.

Three-Network Convergence Policy

In January 2010, the PRC government announced its decision to accelerate the advancement of convergence of telecommunications, television broadcast and Internet access networks to realize interconnection and resource co-sharing among the three networks and further develop the provision of voice, data, television and other services. Specifically, the three-network convergence policy will be initially carried out on a trial basis in selective geographic locations during the period from 2010 to 2012 and further implemented across-the-board in the following three years. In June 2010, the State Council issued the Trial Plan for Three-Network Convergence and called for 12 volunteer regions (cities) and enterprises for the first trial. Following the completion of the first trial in December 2011, the State Council announced 42 additional regions (cities) for the second phase of the trial. In September 2012, we received the Information Network Communicated Audio-Video Program License from the State Administration of Press, Publication, Radio, Film and Television (the "SARFT", formerly, the State Administration of Radio, Film and Television). In August 2015, the General Office of the State Council issued the Notice of Plan of Furthering the Three-Network Convergence, which marked the completion of the trial plan of the three-network convergence and called for furthering the three-network convergence nationwide.

(All Renminbi amounts in millions, except per share data and except otherwise stated)

36. RECONCILIATION OF LIABILITIES ARISING FROM FINANCING ACTIVITIES

The table below details changes in the Group's liabilities arising from financing activities, including both cash and non-cash changes. Liabilities arising from financing activities are those for which cash flows were, or future cash flows will be, classified in the Group's consolidated statement of cash flows as cash flows from financing activities.

	Short-term Debt RMB	Long-term debt and payable RMB	Finance lease obligation RMB	Other payables in respect of the reduction of capital by non-controlling interests RMB	Consideration payable in respect of the Eighth Acquisition (Note 20) RMB	Consideration payable in respect of the acquisition of non-controlling interests (Note 20) RMB	Dividend payable RMB	Total RMB
Balance as of January 1, 2017	40,780	71,646	102	—	—	—	—	112,528
Financing cash flows	13,778	(22,191)	(84)	—	—	(31)	(7,619)	(16,147)
New finance leases	—	—	55	—	—	—	—	55
Interest expenses	—	295	9	—	—	—	—	304
Foreign exchange gain	—	(8)	—	—	—	—	—	(8)
Acquisition of the Eighth Acquired Group	—	—	—	—	87	—	—	87
Acquisition of non-controlling interests	—	—	—	—	—	150	—	150
Distribution to non-controlling interests	—	—	—	—	—	—	89	89
Dividends declared	—	—	—	—	—	—	7,530	7,530
Others	—	—	(5)	—	—	—	—	(5)
Balance as of December 31, 2017	54,558	49,742	77	—	87	119	—	104,583
Financing cash flows	(5,021)	(4,073)	(73)	(20)	(87)	(119)	(7,745)	(17,138)
New finance leases	—	—	200	—	—	—	—	200
Interest expenses	—	304	12	—	—	—	—	316
Foreign exchange loss	—	18	—	—	—	—	—	18
Reduction of capital by non-controlling interests	—	—	—	20	—	—	—	20
Distribution to non-controlling interests	—	—	—	—	—	—	177	177
Dividends declared	—	—	—	—	—	—	7,568	7,568
Balance as of December 31, 2018	49,537	45,991	216	—	—	—	—	95,744

Other than net financing cash outflows for the year ended December 31, 2018 totaling RMB17,138 as presented above, E-surfing Pay, a subsidiary of the Company, received RMB855 in the current year as part of the consideration amounting to RMB945 in respect of contribution from non-controlling interests. The remaining balance of RMB90 as of December 31, 2018 was included in prepayments and other current assets (Note 8).

37. RELATED PARTY TRANSACTIONS

(a) Transactions with China Telecom Group

The Group is a part of companies under China Telecommunications Corporation, a company owned by the PRC government, and has significant transactions and business relationships with members of China Telecom Group.

The principal transactions with China Telecom Group which were carried out in the ordinary course of business are as follows.

	Notes	Year ended December 31, 2016 RMB	2017 RMB	2018 RMB
Construction and engineering services.	(i)	18,936	18,672	16,396
Receiving ancillary services.	(ii)	13,938	16,072	16,744
Interconnection revenues	(iii)	60	48	80
Interconnection charges	(iii)	232	193	204
Receiving community services	(iv)	2,871	3,028	3,296
Net transaction amount of centralized services	(v)	523	727	519
Property lease income	(vi)	36	53	48
Property lease expenses	(vi)	559	654	713
Provision of IT services	(vii)	312	642	531
Receiving IT services	(vii)	1,597	1,812	1,895
Purchases of telecommunications equipment and materials.	(viii)	5,199	4,248	3,760
Sales of telecommunications equipment and materials.	(viii)	2,786	3,291	2,760
Internet applications channel services	(ix)	332	344	298
Interest on amounts due to and loans from China Telecom Group	(x)	2,928	2,720	2,099
Others	(xi)	176	190	186

(All Renminbi amounts in millions, except per share data and except otherwise stated)

39. SHARE APPRECIATION RIGHTS (continued)

In November 2018, the Company approved the granting of 2,394 million share appreciation right units to eligible employees. Under the terms of this grant, all share appreciation rights had a contractual life of five years from date of grant and an exercise price of HK$3.81 per unit. A recipient of share appreciation rights may exercise the rights in stages commencing November 2020. As of each of the third, fourth and fifth anniversary of the date of grant, the total number of share appreciation rights exercisable may not in aggregate exceed 33.3%, 66.7% and 100.0%, respectively, of the total share appreciation rights granted to such person.

During the year ended December 31, 2018 and 2017, no share appreciation right units were exercised. For the year ended December 31, 2018, compensation expense of RMB30 was recognized by the Group in respect of share appreciation rights (2017: Nil).

As of December 31, 2018, the carrying amount of the liability arising from share appreciation rights was RMB30. As of December 31, 2017, no liability arising from share appreciation rights was assumed by the Group.

40. PRINCIPAL SUBSIDIARIES

Details of the Company's subsidiaries which principally affected the results, assets and liabilities of the Group as of December 31, 2018 are as follows:

Name of company	Type of legal entity	Date of incorporation	Place of incorporation and operation	Registered /issued capital (in RMB million unless otherwise stated)	Principal activities
China Telecom System Integration Co., Limited	Limited Company	September 13, 2001	PRC	542	Provision of system integration and consulting services
China Telecom Global Limited	Limited Company	February 25, 2000	Hong Kong Special Administrative Region of the PRC	HK$168 million	Provision of telecommunications services
China Telecom (Americas) Corporation	Limited Company	November 22, 2001	The United States of America	US$43 million	Provision of telecommunications services
China Telecom Best Tone Information Service Co., Limited	Limited Company	August 15, 2007	PRC	350	Provision of Best Tone information services
China Telecom (Macau) Company Limited	Limited Company	October 15, 2004	Macau Special Administrative Region of the PRC	MOP60 million	Provision of telecommunications services
Tianyi Telecom Terminals Company Limited	Limited Company	July 1, 2005	PRC	500	Sales of telecommunications terminals
China Telecom (Singapore) Pte. Limited	Limited Company	October 5, 2006	Singapore	S$1,000,001	Provision of international value-added network services
E-surfing Pay Co., Ltd	Limited Company	March 3, 2011	PRC	500	Provision of e-commerce service
Shenzhen Shekou Telecommunications Company Limited	Limited Company	May 5, 1984	PRC	91	Provision of telecommunications services
China Telecom (Australia) Pty Ltd	Limited Company	January 10, 2011	Australia	AUD1 million	Provision of international value-added network services
China Telecom Korea Co.,Ltd	Limited Company	May 16, 2012	South Korea	KRW500 million	Provision of international value-added network services
China Telecom (Malaysia) SDN BHD	Limited Company	June 26, 2012	Malaysia	MYR3,723,500	Provision of international value-added network services
China Telecom Information Technology (Vietnam) Co., Ltd	Limited Company	July 9, 2012	Vietnam	VND10,500 million	Provision of international value-added network services
iMUSIC Culture & Technology Co., Ltd.	Limited Company	June 9, 2013	PRC	250	Provision of music production and related information services
China Telecom (Europe) Limited	Limited Company	March 2, 2006	The United Kingdom of Great Britain and Northern Ireland	GBP16.15 million	Provision of international value-added network services
Zhejiang Yixin Technology Co., Ltd.	Limited Company	August 19, 2013	PRC	11	Provision of instant messenger service
Tianyi Capital Holding Co., Ltd.	Limited Company	November 30, 2017	PRC	5,000	Capital Investment and provision of consulting services
China Telecom Leasing Corporation Limited.	Limited Company	November 30, 2018	PRC	5,000	Provision of finance lease service

Exhibit 12

Excerpts from China Unicom (Hong Kong) Ltd.'s Form 20-F Annual Report for Fiscal Year 2018

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 20-F

☐ **REGISTRATION STATEMENT PURSUANT TO SECTION 12(b) OR 12(g) OF THE SECURITIES EXCHANGE ACT OF 1934**

OR

☒ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the fiscal year ended December 31, 2018

OR

☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

OR

☐ **SHELL COMPANY REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

Date of event requiring this shell company report _____

For the transition period from _____ to _____

Commission file number 1-15028

CHINA UNICOM (HONG KONG) LIMITED
(Exact Name of Registrant as Specified in Its Charter)

N/A	**Hong Kong**
(Translation of Registrant's Name Into English)	**(Jurisdiction of Incorporation or Organization)**

75th Floor, The Center
99 Queen's Road Central
Hong Kong
(Address of Principal Executive Offices)

Yung Shun Loy Jacky
Telephone: +852 2121 3220
Facsimile: +852 2121 3232
75th Floor, The Center
99 Queen's Road Central
Hong Kong
(Name, Telephone, E-mail and/or Facsimile Number and Address of Company Contact person)

Securities registered or to be registered pursuant to Section 12(b) of the Act:

Title of Each Class	Name of Each Exchange On Which Registered
Ordinary shares	**The New York Stock Exchange, Inc.***

* Not for trading, but only in connection with the listing on The New York Stock Exchange, Inc. of American depositary shares, or ADSs, each representing 10 ordinary shares.

Securities registered or to be registered pursuant to Section 12(g) of the Act:

None
(Title of class)

Securities for which there is a reporting obligation pursuant to Section 15(d) of the Act:

None
(Title of Class)

Indicate the number of outstanding shares of each of the issuer's classes of capital or common stock as of the close of the period covered by the annual report.

As of December 31, 2018, 30,598,124,345 ordinary shares were issued and outstanding.

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ☒ No ☐

If this report is an annual or transition report, indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934. Yes ☐ No ☒

Note – Checking the box above will not relieve any registrant required to file reports pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 from their obligations under those Sections.

Indicate by check mark whether the registrant: (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted pursuant to Rule 405 (§232.405 of this chapter) of Regulation S-T during the preceding 12 months (or for such shorter period that the registrant was required to submit such files). Yes ☒ No ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, or an emerging growth company. See the definitions of "large accelerated filer," "accelerated filer," and "emerging growth company" in Rule 12b-2 of the Exchange Act

Large accelerated filer ☒ Accelerated filer ☐ Non-accelerated filer ☐ Emerging growth company ☐

If an emerging growth company that prepares its financial statements in accordance with U.S. GAAP, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards† provided pursuant to Section 13 (a) of the Exchange Act. ☐

† The term "new or revised financial accounting standard" refers to any update issued by the Financial Accounting Standards Board to its Accounting Standards Codification after April 5, 2012.

Indicate by check mark which basis of accounting the registrant has used to prepare the financial statements included in this filing.

U.S. GAAP ☐ International Financial Reporting Standards as issued by the International Accounting Standards Board ☒ Other ☐

If "Other" has been checked in response to the previous question, indicate by check mark which financial statement item the registrant has elected to follow.

Item 17 ☐ Item 18 ☐

If this is an annual report, indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ☐ No ☒

(APPLICABLE ONLY TO ISSUERS INVOLVED IN BANKRUPTCY PROCEEDINGS DURING THE PAST FIVE YEARS)

Indicate by check mark whether the registrant has filed all documents and reports required to be filed by Sections 12, 13 or 15(d) of the Securities Exchange Act of 1934 subsequent to the distribution of securities under a plan confirmed by a court. Yes ☐ No ☐

	As of or for the year ended December 31,					
	2014	2015	2016	2017	2018	2018
	RMB	RMB	RMB	RMB	RMB	US$[1]
	(in millions, except for per share data)					
Other Financial Data:						
Net cash inflow from operating activities	88,904	84,301	74,593	85,054	92,387	13,437
Net cash outflow from investing activities	(75,319)	(91,354)	(95,749)	(47,336)	(61,179)	(8,898)
Net cash (outflow)/inflow from financing activities	(8,973)	3,427	22,877	(28,414)	(34,058)	(4,954)
Net increase/(decrease) in cash and cash equivalents	**3,802**	**(3,626)**	**1,721**	**9,304**	**(2,850)**	**(415)**
Dividend declared per share	**0.20**	**0.17**	**—**	**0.052**	**0.134**	**0.019**

(1) The translation of RMB into U.S. dollars has been made at the rate of RMB6.8755 to US$1.00, representing the exchange rate as set forth in the H.10 statistical release of the Federal Reserve Board on December 31, 2018. The translations are solely for the convenience of the reader.

(2) Revenue from sales of products associated with the ICT business, which was previously recorded as part of the fixed-line service revenue, has been reclassified as revenue from sales of telecommunications products since 2017 to better reflect the commercial nature of the transactions. The related figures for the years ended December 31, 2014, 2015 and 2016 have been reclassified on the same basis.

(3) See Note 14 to our consolidated financial statements included elsewhere in this annual report on Form 20-F on how basic and diluted earnings per share are calculated under IFRS.

(4) Earnings per ADS is calculated by multiplying earnings per share by 10, which is the number of shares represented by each ADS.

B. Capitalization and Indebtedness

Not Applicable.

C. Reasons for the Offer and Use of Proceeds

Not Applicable.

D. Risk Factors

Risks Relating to Our Business

We face intense competition from other telecommunications operators, including China Mobile and China Telecom, and other companies that provide telecommunications or related services, which may materially and adversely affect our financial condition, results of operations and growth prospects.

The telecommunications industry in China has been evolving. We, along with China Mobile Communications Corporation, or China Mobile, and China Telecommunications Corporation, or China Telecom, are the three full-service telecommunications service providers that operate both fixed-line and mobile telecommunications networks in China. See "A. History and Development of the Company — Restructurings of the Telecommunications Industry" under Item 4. We face intense competition in virtually all aspects of our services, including mobile services, fixed-line voice services, broadband services and data communications services, from China Mobile and China Telecom and expect that this competition will further intensify. In particular, we compete with China Mobile and China Telecom in mobile services. For fixed-line services, we are a leading fixed-line operator in northern China, while China Telecom has a dominant market position in southern China and the MIIT granted to China Mobile the approval for China Mobile to authorize China Mobile Limited to operate the fixed-line telecommunications business in December 2013. In addition, the PRC Government from time to time introduces new policies that may intensify competition among the three telecommunications operators. For example, the PRC government has started mobile number portability pilot programs in certain provinces and cities, and announced in March 2019 to implement the program nationwide in China by the end of 2019. The mobile number portability program allows customers to switch mobile carriers while retaining their numbers, which may intensify the competition among telecommunication operators.

Any failure or delay in expanding and upgrading our mobile networks, any increase in the associated costs (including the costs and expenses that may be incurred as a result of the changes of our marketing and sales policies) could hinder the recovery of our significant capital investment in mobile services, respectively, which could in turn have a material adverse effect on our financial condition, results of operations and growth prospects.

Our business relies on the lease arrangements with the Tower Company as to telecommunications towers and related assets, and we may not be able to achieve the expected benefits from the establishment of the Tower Company and such lease arrangements.

In July 2014, we, China Mobile and China Telecom, the three major telecommunications operators in China, jointly established the Tower Company, which engages primarily in the construction, maintenance and operation of telecommunications towers and other ancillary facilities in China, as well as the provision of maintenance services of base station equipment. In October 2015, the Tower Company acquired all telecommunications towers and related assets from us, China Mobile and China Telecom. In July 2016 and January 2018, we, through our wholly owned subsidiary, CUCL, and the Tower Company entered into a commercial pricing agreement, or the Pricing Agreement, and the supplementary agreement to such Pricing Agreement, or the Supplementary Agreement, respectively, in relation to the leasing of the telecommunications towers and related assets acquired and newly constructed by the Tower Company. In August 2018, the Tower Company completed its initial public offering and listed on the main board of the HKSE and our percentage ownership in the Tower Company decreased to 20.65% as a result. See "A. History and Development of the Company — Establishment of the Tower Company and the Disposal of Telecommunications Towers" under Item 4.

The main purpose for us to participate in the establishment of the Tower Company and lease telecommunications towers and related assets from the Tower Company is to enhance our telecommunications network coverage and capacity, realize long-term investment returns through the equity investment in the Tower Company and reduce capital expenditure as we ceased to construct telecommunications towers on our own. However, because we do not own a majority interest of, or otherwise control, the Tower Company, the Tower Company may not always act in the best interests of us, and there are uncertainties as to whether the services of the Tower Company can sufficiently support our business needs and plans, and whether the Tower Company can fulfill any usage arrangements to be agreed with us and properly operate, maintain and manage its assets.

Furthermore, since it is expected that, in principle, none of us, China Mobile or China Telecom will construct any telecommunications towers in the future, our business will rely on the lease arrangements with the Tower Company. We cannot assure you that we are able to use telecommunications towers and related assets on terms and conditions we desire. The Pricing Agreement, as supplemented and amended from time to time, provides for a pricing adjustment mechanism, which could result in a significant adjustment of the fees charged to us by the Tower Company in the future if there is any significant fluctuation in steel price, inflation and condition of the real estate market. Furthermore, prior to the expiration of lease periods of individual towers, we have to negotiate with the Tower Company new leases of such towers. If we are unable to enter into any new leases or if we are able to enter into new leases but the lease terms are less favorable to us, our business operations, financial condition and results of operations may materially and adversely affected. Failure of the Tower Company to fulfill any usage arrangements with us or properly operate, maintain and manage its telecommunications tower assets or to provide stable services to us could adversely affect the quality and uninterrupted services of our networks, which would in turn materially and adversely affect our business operations as well as our financial condition and results of operations.

We are subject to risks associated with our telecommunications equipment suppliers and other business partners which could be adversely affected by restrictions, sanctions or other legal or regulatory actions under relevant laws and regulations in various jurisdictions which in turn could adversely affect the supply chain and our business operations.

We procure our telecommunications network equipment and related maintenance and technical support from certain PRC and overseas telecommunications equipment suppliers. See "Item 4. Information on the Company—B. Business Overview—Networks." We also transact business with our business partners who may operate globally. As these parties operate globally and are therefore subject to the laws and regulations in various jurisdictions, any restrictions, sanctions or other legal or regulatory actions could cause disruptions or other material difficulties in their business activities to the extent any government of the relevant jurisdictions imposes any restrictions on their import and export activities, or sanctions or other legal or regulatory actions against the suppliers and other business partners in connection with their business activities. The relevant jurisdictions include, among others, the United States, the European Union and the United Nations. Furthermore, as the supply of our telecommunications equipment relies on a global supply chain which is vulnerable to significant disruptions in the supply of parts and other items that are necessary for the relevant manufacturing activities. Such disruptions could prevent those affected suppliers from delivering equipment and services to us in accordance with the agreed terms of supply, which in turn could negatively affect our business operations. For example, we may not be able to find suitable alternative suppliers for the affected equipment in a timely manner. Even if we are able to find alternative suppliers, the commercial terms may not be comparable, and we could therefore be subject to a higher procuring cost. Furthermore, if any of our suppliers raises their prices due to an increase in international trade tariffs, we could be subject to a higher cost in procuring the relevant products. We may experience a significant delay in implementing the part of our business plans that relies on delivery of the affected network equipment and difficulties in timely improving our services that rely on those suppliers for upgrading our networks and related software and applications. Any of these and other consequences could materially adversely affect our business, results of operations, financial condition and prospect and cause a significant volatility in and a decline in our share price.

Because we rely on arrangements with other telecommunications operators, changes to the terms or availability of these arrangements may result in disruptions to our services and operations and may result in customer dissatisfaction and materially and adversely affect our financial condition, results of operations and growth prospects.

Our ability to provide telecommunications services depends upon arrangements with other telecommunications operators. In particular, interconnection is necessary to complete all calls between our subscribers and subscribers of other telecommunications operators. We, either through ourselves or through Unicom Group, have established interconnection and transmission line leasing arrangements with other telecommunications operators, including our parent company, as required to conduct our current business. Any disruption to our interconnection with the networks of those operators or other international telecommunications operators with which we interconnect may affect our operations, service quality and customer satisfaction, thus adversely affecting our business. Furthermore, we are generally not entitled to collect indirect or consequential damages resulting from disruptions in the networks with which we are interconnected. Any disruption in existing interconnection arrangements and transmission line arrangements or any significant change of their terms, as a result of natural events or accidents or for regulatory, technical, competitive or other reasons, may lead to temporary service interruptions and increased costs that can seriously jeopardize our operations and adversely affect our financial condition, results of operations and growth prospects. Difficulties in executing alternative arrangements with other operators on a timely basis and on acceptable terms, including the inability to promptly establish additional interconnection links or increase interconnection bandwidths as required, could also materially and adversely affect our financial condition, results of operations and growth prospects.

Interruptions to our networks and operating systems or to those with which we interconnect, including those caused by natural disaster and service maintenance and upgrades, may disrupt our services and operations and may result in customer dissatisfaction and materially and adversely affect our financial condition, results of operations and growth prospects.

Our network infrastructure and the networks with which we interconnect are vulnerable to potential damages or interruptions from floods, wind, storms, fires, power loss, severed cables, acts of terrorism and similar events. The occurrence of a natural disaster or other unanticipated problems at our facilities or any other failure of our networks or systems, or the networks to which we are interconnected, may result in consequential interruptions in services across our telecommunications infrastructure. In 2018, certain areas of China suffered from natural disasters including typhoons, floods, mountain torrents, mudslides and landslides, and these natural disasters caused extensive damage to our network equipment, including our base stations and optical fiber networks, in the affected areas. As a result, we experienced service stoppage and other disruptions in our operations in those areas and also sustained economic losses. Any future natural disasters may, among other things, significantly disrupt our ability to adequately staff our business, and may generally disrupt our services and operations. Moreover, our networks and systems and the networks with which we interconnect also require regular maintenance and upgrades. Such maintenance and upgrades may cause service disruptions. Network or system failures, as well as abrupt high traffic volumes, may also affect the quality of our services and cause temporary service interruptions. Any such future occurrence may result in customer dissatisfaction and materially and adversely affect our financial condition, results of operations and growth prospects.

In addition, our operations depend on a number of services and facilities provided by Unicom Group. For example, Unicom Group provides us with international gateway services, interconnection services, sales agency and collection services and provision of premises. See "B. Related Party Transactions" under Item 7. The interests of Unicom Group as provider of these services and facilities may conflict with our interests. Failure by Unicom Group to fulfill its obligations under any of these arrangements may have a material adverse effect on our business operations. We currently have limited alternative sources of supply for these services and facilities and, as a result, may have limited ability to negotiate with Unicom Group regarding the terms for providing these services and facilities. Changes in the availability, pricing or quality of these services or facilities may have a material adverse effect on our business and profitability.

The previous internal reorganization of Unicom Group for the A Share offering created a two-step voting mechanism that requires the approval of the minority shareholders of both our Company and China United Network Communications Limited (formerly known as China United Telecommunications Corporation Limited), or the A Share Company, for significant related party transactions between us and Unicom Group.

In October 2002, Unicom Group completed an internal reorganization of its shareholding in our company and the initial public offering in China of its then newly established subsidiary, the A Share Company. As part of this restructuring, a portion of Unicom Group's indirect shareholding in our company was transferred to the A Share Company, whose business is limited to indirectly holding the equity interest of our company without any other direct business operations. A voting mechanism was established to allow public shareholders of the A Share Company to indirectly participate in our shareholders' meetings and a two-step voting mechanism was established for the approval of related party transactions. As a result, any significant related party transaction between us or our subsidiaries and Unicom Group or its other subsidiaries will require the separate approval of the independent minority shareholders of both our company and the A Share Company. Related party transactions approved by our independent minority shareholders nevertheless cannot proceed if they are not approved by the independent minority shareholders of the A Share Company. This adds another necessary step of approval process for those transactions. See "A. History and Development of the Company — Two-Step Voting Arrangements" under Item 4.

The benefits that we expect to enjoy relating to the mixed ownership reform of our ultimate controlling shareholder, Unicom Group, are subject to substantial uncertainty.

As part of the PRC government's efforts to reform state-owned enterprises and increase their competitiveness, our ultimate controlling shareholder, Unicom Group, participated in a pilot program on mixed ownership reform of state-owned enterprises, and implemented a plan to diversify its shareholders' base, or the Mixed Ownership Reform Plan, by bringing in certain strategic investors, including certain large Internet companies, into the A Share Company, our controlling shareholder. See "A. History and Development of the Company – Our Relationship with Unicom Group" and "A. History and Development of the Company — The Mixed Ownership Reform" under Item 4. The main purpose of the Mixed Ownership Reform Plan is to improve the corporate governance, incentive system and management efficiency of the A Share Company, and create synergies through cooperation with strategic investors. However, as there is substantial uncertainty with respect to our cooperation with strategic investors and the improvement in our incentive system, we cannot assure you that these benefits will be achieved as expected.

Investor confidence and the market prices of our shares and ADSs may be materially and adversely impacted if we are or our independent registered public accounting firm is unable to conclude that our internal control over financial reporting is effective in future years as required by Section 404 of the Sarbanes-Oxley Act of 2002.

We are a public company in the United States that is subject to the Sarbanes-Oxley Act of 2002. Pursuant to the requirements of Section 404 of the Sarbanes-Oxley Act of 2002, we have included in this annual report a report of management on our internal control over financial reporting and an attestation report of our independent registered public accounting firm on the effectiveness of our internal control over financial reporting.

China Netcom was incorporated in Hong Kong on October 22, 1999, under the predecessor of the Companies Ordinance as a company limited by shares under the name Target Strong Limited. The company changed its name to China Netcom (Hong Kong) Corporation Limited on December 9, 1999, to China Netcom Corporation (Hong Kong) Limited on August 4, 2000, and to China Netcom Group Corporation (Hong Kong) Limited on July 23, 2004 (the last name change in anticipation of its IPO in 2004).

As part of our integration with China Netcom, our wholly owned subsidiary, CUCL, merged with China Netcom (Group) Company Limited, or CNC China, a wholly owned subsidiary of China Netcom, in January 2009, and upon that merger becoming effective, CUCL assumed all the rights and obligations of CNC China, and all the assets, liabilities and business of CNC China were vested in CUCL. In addition, in January 2009, Unicom Group, our parent company, merged with and absorbed Netcom Group, the parent company of China Netcom. Upon completion of the merger between Unicom Group and Netcom Group, Unicom Group assumed all the rights and obligations of Netcom Group, and all the assets, liabilities and business of Netcom Group have vested in Unicom Group.

Our Relationship with Unicom Group

Our ultimate controlling shareholder is Unicom Group, a company incorporated under the laws of the PRC and majority-owned by the PRC Government. Unicom Group was established in accordance with the State Council's approval to introduce orderly competition in the telecommunications industry in 1994.

Unicom Group transferred certain of its telecommunications assets, rights and liabilities to CUCL (which became our wholly owned subsidiary in China) in April 2000 in preparation for our initial public offering, or IPO. In June 2000, we successfully completed our IPO. Our ordinary shares are listed on the HKSE and our ADSs, each representing 10 of our ordinary shares, are listed on the NYSE.

Unicom Group holds the licenses required for our telecommunications businesses and we derive our rights to operate our businesses from our status as a subsidiary of Unicom Group. Unicom Group undertook to hold and maintain all licenses received from the MIIT in connection with our businesses solely for our benefit during the term of such licenses and at no cost to us. In addition, Unicom Group undertook to take all actions necessary to obtain and maintain for our benefit such governmental licenses or approvals as we shall require to continue to operate our businesses. Unicom Group also agreed not to engage in any business which competes with our businesses other than the then-existing competing businesses of Unicom Group and to grant us a right of first refusal in relation to any government authorization, license or permit, or other business opportunity to develop any new telecommunications technology, product or service. Finally, Unicom Group also gave us an undertaking not to seek an overseas listing for any of its businesses or the businesses of its subsidiaries in which we have engaged or may engage in the future, except through us.

Set forth below is our shareholding structure as of April 16, 2019.

18. INVESTMENTS IN SUBSIDIARIES

As of December 31, 2018, the details of the Company's subsidiaries are as follows:

Name	Place and date of incorporation /establishment and nature of legal entity	Percentage of equity interests held		Particular of issued share capital/paid up capital	Principal activities and place of operation
		Direct	Indirect		
China United Network Communications Corporation Limited ("CUCL")	The PRC, April 21, 2000, limited liability company	100%	—	RMB 213,044,797,828	Telecommunications operation in the PRC
China Unicom Global Limited	Hong Kong, May 29,2015, limited company	100%	—	HKD 2,625,097,491	Investment holding
China Unicom (Hong Kong) Operations Limited	Hong Kong, May 24, 2000, limited company	—	100%	HKD 1,510,100,000	Telecommunications service in Hong Kong
China Unicom (Americas) Operations Limited	USA, May 24, 2002, limited company	—	100%	5,000 shares, USD100 each	Telecommunications service in the USA
China Unicom (Europe) Operations Limited	The United Kingdom, November 8, 2006, limited company	—	100%	4,861,000 shares, GBP1 each	Telecommunications operation in the United Kingdom
China Unicom (Japan) Operations Corporation	Japan, January 25, 2007, limited company	—	100%	1,000 shares, JPY366,000 each	Telecommunications operation in Japan
China Unicom (Singapore) Operations Pte Limited	Singapore, August 5, 2009, limited company	—	100%	30,000,000 shares, RMB1 each	Telecommunications operation in Singapore
China Unicom (South Africa) Operations (Pty) Limited	South Africa, November 19, 2012, limited liability company	—	100%	100 shares, ZAR 1 each	Telecommunications operation in South Africa
China Unicom (MYA) Operations Company Limited	The Republic of the Union of Myanmar ("Myanmar"), June 7, 2013, limited liability company	30%	70%	2,150,000 shares, USD1 each	Communications technology training in Myanmar
China Unicom (Australia) Operations Pty Limited	Australia, May 27, 2014, limited liability company	—	100%	4,350,000 shares, AUD 1 each	Telecommunications operation in Australia
China Unicom (Russia) Operations Limited Liability Company	Russia, December 28, 2016, limited liability company	—	100%	RUB10,000	Telecommunications service in Russia

Exhibit 13

"Nokia Corp., Nokia and China Huaxin Sign Definitive Agreements for Creation of New Nokia Shanghai Bell Joint Venture"

NOKIA

Nokia and China Huaxin sign definitive agreements for creation of new Nokia Shanghai Bell joint venture

Nokia Corporation
Stock Exchange Release
May 18, 2017 at 09:00 (CET +1)

Nokia and China Huaxin sign definitive agreements for creation of new Nokia Shanghai Bell joint venture

Beijing, China - Nokia and China Huaxin Post & Telecommunication Economy Development Center ("China Huaxin") today signed the definitive agreements of the proposed integration of Alcatel-Lucent Shanghai Bell Co. Ltd. (ASB) and Nokia's China business. The new joint venture will be branded as Nokia Shanghai Bell (NSB).

As a result of today's announcement, the joint venture will become Nokia's exclusive platform in China for the continued development of new technologies in areas like IP routing, optical, fixed and next-generation 5G; and with the support of Nokia, NSB will continue to look for opportunities in select overseas markets.

ASB and Nokia's China business have been effectively operating as one entity since January 2016 when an interim operational agreement was signed.

The closing of today's agreement, targeted to happen in July 2017, is subject to various customary administrative, legal, regulatory and other conditions. Nokia will own 50% plus one share of NSB, with China Huaxin owning the remainder, and the new joint venture will have one board of directors and one management team.

NSB will represent the major part of Nokia's overall Greater China business and fully leverage both shareholders' strengths, including innovation, global scale, efficiency and a deep understanding of the local market; and with the aim of increasing Nokia's market presence in China. It will further Nokia's strategic goals of leading in high-performance networks with communication service providers and expanding to new vertical markets in enterprise, public sector, and cloud/internet companies.

NSB research and development (R&D) will be an integral part of Nokia's global R&D community, with a total of around 16 000 personnel, including 10 000 researchers, working across six R&D sites in China. It will maintain and further enhance Nokia's world-class product and research capabilities in areas that include 5G, IoT and Cloud.

NSB's R&D scope and activities will be carried out according to Nokia's applicable policies, global R&D processes and product roadmaps. NSB will also support strategic initiatives of the Chinese government and engage in long-term research projects aligned with and implementing Nokia Bell Labs' Future X Network.

Rajeev Suri, President and CEO of Nokia Corporation, said: "Today's agreement is historic for Nokia and for China, marking the next step of our decades-long commitment to the country and underscoring China's leading role in developing next-generation communication technologies. Nokia Shanghai Bell will enhance our ability to innovate, helping us strengthen ties with communication service providers and expand to new, fast-growing sectors in need of high-performing networks."

Yuan Xin, General Manager of China Huaxin, said: "We are fully confident in the new joint venture's success during the industry transformation brought by the new technologies like 5G and IoT. The successful combination globally and in China brings together the leading E2E network technologies and most powerful innovation engines from both sides. We're excited to work with Nokia to establish a future-oriented innovative technology company, with a win-win cooperative model for the bigger success in the new era."

About China Huaxin

China Huaxin Post and Telecommunication Economy Development Center is an industrial investment company that seeks long-term commercial growth opportunities in the Information and Communications Technologies (ICT) sector. China Huaxin has extensive global operations and international investment experience. China Huaxin aspires to be a competitive global industry holding group that creates long-term value for its stakeholders and for society as a whole by nurturing and advancing technology innovation in the Information Industry. www.sinohx.com

About Nokia

We create the technology to connect the world. Powered by the research and innovation of Nokia Bell Labs, we serve communications service providers, governments, large enterprises and consumers, with the industry's most complete, end-to-end portfolio of products, services and licensing. From the enabling infrastructure for 5G and the Internet of Things, to emerging applications in virtual reality and digital health, we are shaping the future of technology to transform the human experience. www.nokia.com

Media Inquiries

Nokia China Communications
LING Yi
T: +86 21 38436561
M: +86 18616388716
yi.a.ling@alcatel-sbell.com.cn

Nokia Corporate Communications
T: +358 10 448 4900
press.services@nokia.com

FORWARD-LOOKING STATEMENTS

It should be noted that Nokia and its businesses are exposed to various risks and uncertainties and certain statements herein that are not historical facts are forward-looking statements, including, without limitation, those regarding: A) our ability to integrate Alcatel Lucent into our operations and achieve the targeted business plans and benefits, including targeted synergies in relation to the acquisition of Alcatel Lucent; B) expectations, plans or benefits related to our strategies and growth management; C) expectations, plans or benefits related to future performance of our businesses; D) expectations, plans or benefits related to changes in organizational and operational structure; E) expectations regarding market developments, general economic conditions and structural changes; F) expectations and targets regarding financial performance, results, operating expenses, taxes, currency exchange rates, hedging, cost savings and competitiveness, as well as results of operations including targeted synergies and those related to market share, prices, net sales, income and margins; G) timing of the deliveries of our products and services; H) expectations and targets regarding collaboration and partnering arrangements, joint ventures or the creation of joint ventures, including the creation of the new Nokia Shanghai Bell joint venture and the related administrative, legal, regulatory and other conditions, as well as our expected customer reach; I) outcome of pending and threatened litigation, arbitration, disputes, regulatory proceedings or investigations by authorities; J) expectations regarding restructurings, investments, uses of proceeds from transactions, acquisitions and divestments and our ability to achieve the financial and operational targets set in connection with any such restructurings, investments, divestments and acquisitions; and K) statements preceded by or including "believe," "expect," "anticipate," "foresee," "sees," "target," "estimate," "designed," "aim," "plans," "intends," "focus," "continue," "project," "should," "will" or similar expressions. These statements are based on management's best assumptions and beliefs in light of the information currently available to it. Because they involve risks and uncertainties, actual results may differ materially from the results that we currently expect. Factors, including risks and uncertainties that could cause these differences include, but are not limited to: 1) our ability to execute our strategy, sustain or improve the operational and financial performance of our business and correctly identify and successfully pursue business opportunities or growth; 2) our ability to achieve the anticipated benefits, synergies, cost savings and efficiencies of the acquisition of Alcatel Lucent, and our ability to implement our organizational and operational structure efficiently; 3) general economic and market conditions and other developments in the economies where we

operate; 4) competition and our ability to effectively and profitably compete and invest in new competitive high-quality products, services, upgrades and technologies and bring them to market in a timely manner; 5) our dependence on the development of the industries in which we operate, including the cyclicality and variability of the information technology and telecommunications industries; 6) our global business and exposure to regulatory, political or other developments in various countries or regions, including emerging markets and the associated risks in relation to tax matters and exchange controls, among others; 7) our ability to manage and improve our financial and operating performance, cost savings, competitiveness and synergies after the acquisition of Alcatel Lucent; 8) our dependence on a limited number of customers and large multi-year agreements; 9) exchange rate fluctuations, as well as hedging activities; 10) Nokia Technologies' ability to protect its IPR and to maintain and establish new sources of patent licensing income and IPR-related revenues, particularly in the smartphone market; 11) our dependence on IPR technologies, including those that we have developed and those that are licensed to us, and the risk of associated IPR-related legal claims, licensing costs and restrictions on use; 12) our exposure to direct and indirect regulation, including economic or trade policies, and the reliability of our governance, internal controls and compliance processes to prevent regulatory penalties in our business or in our joint ventures; 13) our ability to identify and remediate material weaknesses in our internal control over financial reporting; 14) our reliance on third-party solutions for data storage and service distribution, which expose us to risks relating to security, regulation and cybersecurity breaches; 15) inefficiencies, breaches, malfunctions or disruptions of information technology systems; 16) Nokia Technologies' ability to generate net sales and profitability through licensing of the Nokia brand, particularly in digital media and digital health, and the development and sales of products and services, as well as other business ventures which may not materialize as planned; 17) our exposure to various legislative frameworks and jurisdictions that regulate fraud and enforce economic trade sanctions and policies, and the possibility of proceedings or investigations that result in fines, penalties or sanctions; 18) adverse developments with respect to customer financing or extended payment terms we provide to customers; 19) the potential complex tax issues, tax disputes and tax obligations we may face in various jurisdictions, including the risk of obligations to pay additional taxes; 20) our actual or anticipated performance, among other factors, which could reduce our ability to utilize deferred tax assets; 21) our ability to retain, motivate, develop and recruit appropriately skilled employees; 22) disruptions to our manufacturing, service creation, delivery, logistics and supply chain processes, and the risks related to our geographically-concentrated production sites; 23) the impact of litigation, arbitration, agreement-related disputes or product liability allegations associated with our business; 24) our ability to optimize our capital structure as planned and re-establish our investment grade credit rating or otherwise improve our credit ratings; 25) our ability to achieve targeted benefits from or successfully achieve the required administrative, legal, regulatory and other conditions and implement planned transactions, including the creation of the new Nokia Shanghai Bell joint venture, as well as the liabilities related thereto; 26) our involvement in joint ventures and jointly-managed companies; 27) the carrying amount of our goodwill may not be recoverable; 28) uncertainty related to the amount of dividends and equity return we are able to distribute to shareholders for each financial period; 29) pension costs, employee fund-related costs, and healthcare costs; and 30) risks related to undersea infrastructure, as well as the risk factors specified on pages 67 to 85 of our 2016 annual report on Form 20-F under "Operating and financial review and prospects-Risk factors" and in our other filings with the U.S. Securities and Exchange Commission. Other unknown or unpredictable factors or underlying assumptions subsequently proven to be incorrect could cause actual results to differ materially from those in the forward-looking statements. We do not undertake any obligation to publicly update or revise forward-looking statements, whether as a result of new information, future events or otherwise, except to the extent legally required.

End of the release / See all releases

Nokia press subscription

First name*

Last name*

Country*

E-mail*

Subscribe

*required information

Enquiries on this topic

Media enquiries

press.services@nokia.com

Tel. +358 10448 4900

Helsinki · Evening GMT +2 / CEST

Investor enquiries

investor.relations@nokia.com

Tel. +358 40 803 4080

Helsinki · Evening GMT +3 / EEST

Stock exchange releases

Updated: 21.05.2019 · 18:30 EEST

1 / 8

21 May 2019

Resolutions of the Nokia Annual General Meeting 2019; the Board of Directors resolved to distribute EUR 0.05 per share as the first instalment of dividend

25 Apr 2019

Nokia Corporation Interim Report for Q1 2019

18 Apr 2019

Nokia provides reca segment results an disclosures for 201 financial reporting s

Exhibit 14

"Finnish Visit to Nokia Shanghai Bell"

BUSINESS NEWS, CHINA, FINLAND, TELECOMMUNICATIONS

Finnish visit to Nokia Shanghai Bell

by Joakim Persson • October 12, 2018 • 0 Comments

Team Finland led by **Consul General Jan Wahlberg** on 10 October visited the R&D Center at **Nokia Shanghai Bell** to discuss future cooperation.

This Shanghai lab plays a unique role in building Nokia's research eco-system in China by establishing extensive cooperation between Chinese customers and top universities in China for national key projects and consortium.

Nokia Shanghai Bell is a joint venture between Nokia and China Huaxin, integrating Alcatel-Lucent Shanghai Bell Co. Ltd and Nokia's China business. The joint venture, which started its operation in July 2017, is Nokia's exclusive platform in China for the continued development of new technologies such as IP routing, optical, fixed and next-generation 5G. The facility is located in Jinqiao, east of Shanghai, and is ranked as a top 10 enterprise research center in China.

Nokia's research and development staff in China is altogether around 10 000 people in six different locations. They work as an integral part of the global Nokia R&D team.

The research team is dedicated to pioneering research in a vast array of technologies including: Wireless access and fixed access technology; 5G, advanced multiple antenna technologies; Device to device communication; Cloud RAN; Green

radio; Small cell technology; TDD specific technologies; LTE-A/beyond broadcast/multicast; Cellular based machine to machine; Software-defined converged access network; Next generation PON; and RoF-based fronthaul

Sources: Nokia Shanghai Bell, Consulate General of Finland in Shanghai

Related Posts

Finnish Minister Olli Rehn visited Shanghai

Finnish design firms in Shanghai relocated

Exhibit 15

"NSA Concerns Give Chinese Server Maker a Boost"

TECHNOLOGY

NSA Concerns Give Chinese Server Maker a Boost

Inspur Is Taking Market Share From IBM, Other U.S. Rivals in China in Wake of Snowden Revelations

By Eva Dou

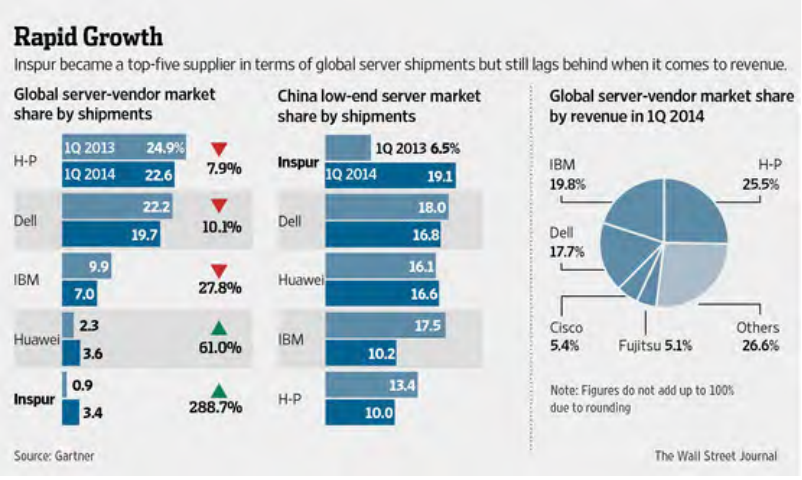
July 29, 2014 1:10 p.m. ET

BEIJING—A Chinese company that once made computer accessories is seeking to rival International Business Machines Corp. as a top provider of big-ticket computer servers in China.

Its strategy, in part: Bring up Edward Snowden.

Inspur Group Co. is using Chinese worries about U.S. gear as part of its effort to take market share from IBM, Hewlett-Packard Co. and other foreign rivals. U.S. technology companies fell under a cloud in China last year after the former U.S. National Security Agency contractor disclosed that the U.S. government was collecting sensitive data from American companies.

Inspur Chairman Sun Pishu, a member of the country's legislature, proposed measures this year to review critical technology purchases and accelerate the shift toward homegrown gear. The company unveiled a marketing program called I2I—IBM to Inspur—aimed at convincing businesses to switch from Big Blue.



Since the NSA controversy began, Inspur, which started out in the 1960s making computer accessories in China's northeast Shandong province, has seen domestic server sales soar. It overtook Dell Inc., China's Huawei Technologies Co. and H-P in the first quarter to top China's charts for server shipments, according to data from researcher Gartner.

The boom in China has also lifted Inspur to the No. 5 spot globally. U.S. vendors Dell, H-P and IBM all saw market-share declines in China and globally during the same period.

A spokesman for Dell declined to comment. Representatives at IBM and H-P didn't respond to a request for comment.

But neither Inspur nor Huawei are in the top five list globally when it comes to revenue, and even in China, they lag behind their U.S. rivals. That means foreign companies still have a firm hold on the market for the most sophisticated and expensive machines needed to run the country's big banks and other important areas, Gartner says.

RELATED

- Microsoft, the 'Guardian Warriors' and China's Cybersecurity Fears

Inspur's rapid growth showcases the successes and challenges for Beijing's long-running push to shed its dependence on the likes of IBM, Oracle Corp., Cisco Systems Inc. and other Western companies for high-tech equipment. China eventually hopes to replace Western equipment running the critical functions in major state-run banks and other government-controlled companies, though experts say that day is far off.

Beijing's push has been accelerated by rising tensions between the U.S. and China over cybersecurity threats. In recent months, major U.S. tech firms like Apple Inc. and Microsoft Corp. have been in the cross hairs of Chinese state media, which questioned the security of their technologies.

China is also pursuing antitrust investigations of both Microsoft and Qualcomm this year, showing that its officials are taking a harder line against foreign firms.

China has worked for decades to develop homegrown technologies to wean itself off its dependence on U.S. firms. Since 1986, the government has used something called the 863 Program to fund technology development in sectors deemed strategic, ranging from spacecraft to automation. Most recently, the country is pouring $5 billion into its microchip industry, as well as encouraging the development of homegrown software to compete with Microsoft's Windows and Google Inc.'s Android.

Inspur, which developed China's first pager in 1990 and first server three years later, has played a key role in the government plans. Its chairman Mr. Sun, nicknamed "the father of Chinese servers," is a member of the 863 Program's expert committee. The company worked with China's National University of Defense Technology to build the world's fastest supercomputer, China's Tianhe-2, on an 863 Program grant.

Inspur also received a 1 billion yuan ($162 million) grant under the same government program in 2009 to develop China's first high-end server. The result, Inspur's K1 Tiansuo, began sales in 2010 and remains the company's most advanced server.

Still, experts say China's server makers don't yet have the capability to make mainframes, the most advanced type of servers, and their successes are mainly due to lower prices and better device customization. "We think our customers at the end of the day make their purchase decisions based on value," said Zhang Haitao, Inspur's vice president.

An executive at one of China's biggest state-run banks said the lender's core functions run almost exclusively on foreign equipment. "It's not like cellphones," the executive said. "You can't just switch them."

IDC analyst Thomas Zhou estimates that 90% of Chinese banks' $800 million of server purchases this year will go to U.S. vendors. So far, he says, Chinese banks use locally made servers for simpler tasks such as running the software that interacts with consumers online and at kiosks.

Political factors are also driving some sales of Chinese servers, analysts say, noting that politically connected Inspur has been particularly adept at leveraging them.

"Since the end of 2012, the Chinese government has encouraged large state-owned enterprises and the government sector to buy more servers from local vendors," said Gartner analyst Uko Tian.

Shandong State-Owned Assets Investment Holdings Co. owns a controlling stake in Inspur Group. The company's server-making unit, Inspur Electronic Information Industry Co. , is publicly traded on the Shenzhen stock exchange. In March, Mr. Sun, Inspur's chairman, brought forth several proposals to the National People's Congress, where he holds a seat. One proposal was to accelerate a switch to domestically made technologies, including Inspur's K1 Tiansuo server. Another was to conduct mandatory security approvals for the suppliers of "critical information infrastructure," whose definition would be expanded to include the telecom, finance, energy and transportation industries.

In May, in the wake of U.S. charges against five Chinese military officers for spying, China's State Internet Information Office said the government would establish procedures to evaluate the security of Internet technology and services in sectors related to national security.

China's President Xi Jinping reiterated the government's commitment to developing its own technology in June, saying that science and technology were the foundation of national strength.

Unlike Inspur, Huawei has tried to shy away from the national-security issue as it tries to build out its international business—and is itself facing scrutiny in the U.S. over national-security concerns. Zheng Yelai, president of Huawei's IT product line, said in an interview he believes the company's recent sales growth in China was due to its competitive products rather than the Snowden disclosures.

Inspur's Mr. Zhang says the spying concerns have likely had some help to sales, although he wouldn't say how much.

"Customers surely have this concern," he said. "But whether they are buying because of this reason is hard to say."

—Lingling Wei contributed to this article.

Write to Eva Dou at eva.dou@wsj.com

Exhibit 16

PC Magazine's Online Product-Overview Page for Cisco Systems, Inc.'s Catalyst 3650-48P Layer 3 Switch

Cisco Catalyst 3650-48P Layer 3 Switch

$6,361.99

FREE Shipping

ADD TO CART

Product Overview

UPC Code: 882658593314
Manufacturer Warranty: Limited Lifetime
Country of Origin: CHINA

General Information

Manufacturer: Cisco Systems, Inc
Manufacturer Part Number: WS-C3650-48PS-S
Manufacturer Website Address: www.cisco.com
Brand Name: Cisco
Product Line: Catalyst
Product Series: 3650
Product Model: 3650-48P
Product Name: Catalyst 3650-48P Layer 3 Switch
Marketing Information:
The Cisco Catalyst® 3650 Series is the next generation of enterprise-class standalone and stackable access-layer switches that provide the foundation for full convergence between wired and wireless on a single platform. The Cisco Catalyst 3650 is built on the advanced Cisco StackWise®-160, and takes advantage of the new Cisco® Unified Access Data Plane (UADP) application-specific integrated circuit (ASIC). This switch can enable uniform wired-wireless policy enforcement, application visibility, flexibility, application optimization, and superior resiliency. The Cisco Catalyst 3650 Series Switches support full IEEE 802.3at Power over Ethernet Plus (PoE+), and offer modular and field-replaceable redundant fans and power supplies. They can help you increase wireless productivity and reduce your TCO.

Product Type: Layer 3 Switch

Interfaces/Ports

Total Number of Network Ports: 48
Token Ring Port: No
LRE Port: No
Uplink Port: Yes
Bypass: No
Modular: No
Management Port: Yes
Number of PoE+ (RJ-45) Ports: 48
Stack Port: Yes
Port/Expansion Slot Details: 4 x Gigabit Ethernet Uplink
Port/Expansion Slot Details: 48 x Gigabit Ethernet Network

Media & Performance

Media Type Supported: Twisted Pair
Twisted Pair Cable Standard: Category 5e
Ethernet Technology: Gigabit Ethernet
Network Technology: 10/100/1000Base-T

I/O Expansions

Number of Total Expansion Slots: 4
Expansion Slot Type: SFP
Number of SFP Slots: 4

Network & Communication

Layer Supported: 4

Management & Protocols

Manageable: Yes
Management:

- QoS
- VLAN

- Embedded Event Manager (EEM)
- RMON
- SNMP v1, 2c, 3
- MIB
- DHCP

Memory

Standard Memory: 4 GB
Memory Technology: DRAM
Flash Memory: 2 GB

Reliability

MTBF: 383760 Hour

Power Description

PoE (RJ-45) Port: No
Input Voltage: 110 V AC
Input Voltage: 220 V AC
Power Source: Power Supply
Redundant Power Supply Supported: Yes

Physical Characteristics

Compatible Rack Unit: 1U
Form Factor: Rack-mountable
Form Factor: Desktop
Height: 1.7"
Width: 17.5"
Depth: 17.6"
Weight (Approximate): 16.75 lb

Miscellaneous

System Requirements:

- Processor Speed: 233 MHz minimum
- DRAM: 512 MB
- Number of Colors: 256
- Resolution: 1024 x 768
- Font Size: Small

Operating Systems:

- Windows XP
- Windows 7
- Mac OS X

Web Browsers:

- Google Chrome
- Microsoft Internet Explorer
- Mozilla Firefox

Warranty

Limited Warranty: Lifetime

Related Products

Cisco Catalyst 2960X-48FPS-L Ethernet Switch

Cisco Catalyst 2960X-48LPS-L Ethernet Switc

$3,704.99 $3,144.99

← BACK TO NETWORKING

View All Categories

Exhibit 17

Excerpts from Cisco Systems, Inc.'s Form 10-K Annual Report for Fiscal Year Ended July 30, 2016

Table of Contents

UNITED STATES SECURITIES AND EXCHANGE COMMISSION

WASHINGTON, D.C. 20549

FORM 10-K

(Mark one)

☒ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**
For the fiscal year ended July 30, 2016

or

☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**
For the transition period from ____ to ____

Commission file number 0-18225

CISCO SYSTEMS, INC.

(Exact name of Registrant as specified in its charter)

California	**77-0059951**
(State or other jurisdiction of incorporation or organization)	**(IRS Employer Identification No.)**
170 West Tasman Drive San Jose, California	**95134-1706**
(Address of principal executive offices)	**(Zip Code)**

Registrant's telephone number, including area code: (408) 526-4000
Securities registered pursuant to Section 12(b) of the Act:

Title of Each Class:	**Name of Each Exchange on which Registered**
Common Stock, par value $0.001 per share	The NASDAQ Stock Market LLC

Securities registered pursuant to Section 12(g) of the Act: None

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. ☒ Yes ☐ No

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act. ☐ Yes ☒ No

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. ☒ Yes ☐ No

Indicate by check mark whether the registrant has submitted electronically and posted on its corporate Web site, if any, every Interactive Data File required to be submitted and posted pursuant to Rule 405 of Regulation S-T (§232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit and post such files). ☒ Yes ☐ No

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K is not contained herein, and will not be contained to the best of registrant's knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K. ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, or a smaller reporting company. See definitions of "large accelerated filer," "accelerated filer" and "smaller reporting company" in Rule 12b-2 of the Exchange Act.

Large accelerated filer	☒	Accelerated filer	☐
Non-accelerated filer	☐ (Do not check if a smaller reporting company)	Smaller reporting company	☐

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). ☐ Yes ☒ No

Aggregate market value of registrant's common stock held by non-affiliates of the registrant, based upon the closing price of a share of the registrant's common stock on January 22, 2016 as reported by the NASDAQ Global Select Market on that date: $117,979,166,007

Number of shares of the registrant's common stock outstanding as of September 2, 2016 : 5,014,353,833

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the registrant's Proxy Statement relating to the registrant's 2016 Annual Meeting of Shareholders, to be held on December 12 , 2016, are incorporated by reference into Part III of this Annual Report on Form 10-K where indicated.

Acquisitions

We have acquired many companies, and we expect to make future acquisitions. Mergers and acquisitions of high-technology companies are inherently risky, especially if the acquired company has yet to ship a product. No assurance can be given that our previous or future acquisitions will be successful or will not materially adversely affect our financial condition or operating results. Prior acquisitions have resulted in a wide range of outcomes, from successful introduction of new products and technologies to an inability to do so. The risks associated with acquisitions are more fully discussed in "Item 1A. Risk Factors," including the risk factor entitled "We have made and expect to continue to make acquisitions that could disrupt our operations and harm our operating results."

Investments in Privately Held Companies

We make investments in privately held companies that develop technology or provide services that are complementary to our products or that provide strategic value. The risks associated with these investments are more fully discussed in "Item 1A. Risk Factors," including the risk factor entitled "We are exposed to fluctuations in the market values of our portfolio investments and in interest rates; impairment of our investments could harm our earnings."

Strategic Alliances

We pursue strategic alliances with other companies in areas where collaboration can produce industry advancement and acceleration of new markets. The objectives and goals of a strategic alliance can include one or more of the following: technology exchange, product development, joint sales and marketing, or new market creation. Companies with which we have, or recently had, strategic alliances include the following:

Accenture Ltd; Apple Inc.; AT&T Inc.; Cap Gemini S.A.; Citrix Systems, Inc.; EMC Corporation; LM Ericsson Telephone Company; Fujitsu Limited; Inspur Group Ltd.; Intel Corporation; International Business Machines Corporation; Italtel SpA; Johnson Controls Inc.; Microsoft Corporation; NetApp, Inc.; Oracle Corporation; Red Hat, Inc.; SAP AG; Sprint Nextel Corporation; Tata Consultancy Services Ltd.; VCE Company, LLC ("VCE"); VMware, Inc.; Wipro Limited; and others.

Companies with which we have strategic alliances in some areas may be competitors in other areas, and in our view this trend may increase. The risks associated with our strategic alliances are more fully discussed in "Item 1A. Risk Factors," including the risk factor entitled "If we do not successfully manage our strategic alliances, we may not realize the expected benefits from such alliances, and we may experience increased competition or delays in product development."

Competition

We compete in the networking and communications equipment markets, providing products and services for transporting data, voice, and video traffic across intranets, extranets, and the Internet. These markets are characterized by rapid change, converging technologies, and a migration to networking and communications solutions that offer relative advantages. These market factors represent both an opportunity, and a competitive threat to us. We compete with numerous vendors in each product category. The overall number of our competitors providing niche product solutions may increase. Also, the identity and composition of competitors may change as we increase our activity in our new product markets. As we continue to expand globally, we may see new competition in different geographic regions. In particular, we have experienced price-focused competition from competitors in Asia, especially from China, and we anticipate this will continue.

Our competitors include Amazon Web Services LLC; Arista Networks, Inc.; ARRIS Group, Inc.; Avaya Inc.; Blue Jeans Networks, Brocade Communications Systems, Inc.; Check Point Software Technologies Ltd.; Citrix Systems, Inc.; Dell Inc.; Extreme Networks, Inc.; F5 Networks, Inc.; FireEye, Inc.; Fortinet, Inc.; Hewlett-Packard Enterprise Company; Huawei Technologies Co., Ltd.; International Business Machines Corporation; Juniper Networks, Inc.; Lenovo Group Limited; Microsoft Corporation; Nokia Corporation; Palo Alto Networks, Inc.; Polycom, Inc.; Riverbed Technology, Inc.; Symantec Corporation; Ubiquiti Networks and VMware, Inc.; among others.

Some of these companies compete across many of our product lines, while others are primarily focused in a specific product area. Barriers to entry are relatively low, and new ventures to create products that do or could compete with our products are regularly formed. In addition, some of our competitors may have greater resources, including technical and engineering resources, than we do. As we expand into new markets, we will face competition not only from our existing competitors but also from other competitors, including existing companies with strong technological, marketing, and sales positions in those markets. We also sometimes face competition from resellers and distributors of our products. Companies with which we have strategic alliances in some areas may be competitors in other areas, and in our view this trend may increase. For example, the enterprise data center is undergoing a fundamental transformation arising from the convergence of technologies, including computing, networking, storage, and software, that previously were segregated within the data center. Due to several factors, including the availability of highly scalable and general purpose microprocessors, application-specific integrated circuits offering advanced services, standards-based protocols, cloud computing, and virtualization, the convergence of technologies within the enterprise data center is spanning multiple,

Exhibit 18

Excerpts from Hewlett Packard Enterprise Co.'s Form 10-K Annual Report for Fiscal Year Ended Oct. 31, 2018

Table of Contents

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 10-K

(Mark One)

☒ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the fiscal year ended October 31, 2018
Or

☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the transition period from to

Commission file number 001-37483

HEWLETT PACKARD ENTERPRISE COMPANY
(Exact name of registrant as specified in its charter)

Delaware	**47-3298624**
(State or other jurisdiction of incorporation or organization)	(I.R.S. employer identification no.)
3000 Hanover Street, Palo Alto, California	**94304**
(Address of principal executive offices)	(Zip code)

Registrant's telephone number, including area code: **(650) 687-5817**
Securities registered pursuant to Section 12(b) of the Act:

Title of each class	Name of each exchange on which registered
Common stock, par value $0.01 per share	New York Stock Exchange

Securities registered pursuant to Section 12(g) of the Act:
None

Indicate by check mark if the registrant is a well-known seasoned issuer as defined in Rule 405 of the Securities Act. Yes ☒ No ☐

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act. Yes ☐ No ☒

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically and posted on its corporate Web site, if any, every Interactive Data File required to be submitted and posted pursuant to Rule 405 of Regulation S-T during the preceding 12 months (or for such shorter period that the registrant was required to submit and post such files). Yes ☒ No ☐

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K is not contained herein, and will not be contained, to the best of registrant's knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K. ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, a smaller reporting company, or an emerging growth company. See the definitions of "large accelerated filer," "accelerated filer", "smaller reporting company" and "emerging growth company" in Rule 12b-2 of the Exchange Act. (Check one):

Large accelerated filer ☒	Accelerated filer ☐	Non-accelerated filer ☐ (Do not check if a smaller reporting company)	Smaller reporting company ☐
			Emerging growth company ☐

HPE StoreOnce and HPE Recovery Manager Central, solutions for secondary workloads and traditional tape, storage networking and disk products, such as HPE MSA and HPE XP.

- *DC Networking.* Our offerings include top-of-rack switches, core switches, and open networking switches. We offer a full stack of networking solutions that deliver open, scalable, secure and agile solutions, by enabling programmable fabric, network virtualization, and network management products.

- HPE Pointnext creates preferred IT experiences that power the digital business. The HPE Pointnext team and our extensive partner network provide value across the IT life cycle delivering advice, transformation projects, professional services, support services and operational services for Hybrid IT and the Intelligent Edge. HPE Pointnext is also a provider of on-premises flexible consumption models, such as HPE GreenLake, that enable IT agility, simplify operations and align cost to business value. HPE Pointnext offerings includes Operational Services, Advisory and Professional Services, and Communication and Media Solutions ("CMS").

Intelligent Edge

The Intelligent Edge business is comprised of enterprise networking and security solutions for businesses of any size, offering secure connectivity for campus and branch environments, operating under the Aruba brand. The primary business drivers for Intelligent Edge solutions are mobility and IoT.

- *HPE Aruba Product* includes wired and wireless local area network hardware products such as Wi-Fi access points, switches, routers, sensors, and software products that include network management, network access control, analytics and assurance, and location services software .
- *HPE Aruba Services* offers professional and support services for the Intelligent Edge portfolio of products.

Financial Services

Financial Services provides flexible investment solutions, such as leasing, financing, IT consumption, and utility programs and asset management services, for customers that facilitate unique technology deployment models and the acquisition of complete IT solutions, including hardware, software and services from Hewlett Packard Enterprise and others. In order to provide flexible services and capabilities that support the entire IT life cycle, FS partners with customers globally to help build investment strategies that enhance their business agility and support their business transformation. FS offers a wide selection of investment solution capabilities for large enterprise customers and channel partners, along with an array of financial options to SMBs and educational and governmental entities.

Corporate Investments

Corporate Investments includes Hewlett Packard Labs and certain business incubation projects.

Our Strengths

We believe that we possess a number of competitive advantages that distinguish us from our competitors, including:

Strong solutions portfolio for the data center, cloud and intelligent edge . We combine our software-defined infrastructure and services capabilities to provide what we believe is the strongest portfolio of enterprise solutions in the IT industry. Our ability to deliver a comprehensive IT strategy-from the cloud to the data center to the intelligent edge, through our high-quality products and high-value consulting and support services in a single package-is one of our principal differentiators.

Multi-year innovation roadmap . We have been in the technology and innovation business for over 75 years. Our vast intellectual property portfolio and global research and development capabilities are part of a broader innovation roadmap designed to help organizations take advantage of the expanding amount of data available and leverage the latest technology developments like cloud, artificial intelligence, and cybersecurity to drive business outcomes now and in the future.

Global distribution and partner ecosystem . We are experts in delivering innovative technological solutions to our customers in complex multi-country, multi-vendor and/or multi-language environments. We have one of the largest go-to-market capabilities in our industry, including a large ecosystem of channel partners, which enables us to market and deliver our product offerings to customers located virtually anywhere in the world.

Custom financial solutions . We have developed innovative financing solutions and IT consumption models to facilitate the delivery of our products and services to our customers. We deliver flexible investment solutions and expertise that help customers and other partners create unique technology deployments based on specific business needs.

costs and expenses, and require substantial expenditures and recovery time in order to fully resume operations. Our corporate headquarters and a portion of our research and development activities are located in California, which has suffered from drought conditions and catastrophic wildfires affecting the health and safety of our employees. Other critical business operations and some of our suppliers are located in California and Asia, near major earthquake faults known for seismic activity. In addition, our principal worldwide IT data centers are located in the southern United States, making our operations more vulnerable to climate-related natural disasters, such as 2017 hurricane Harvey, which caused severe damage in Houston. The manufacture of product components, the final assembly of our products and other critical operations are concentrated in certain geographic locations, including the Czech Republic, Mexico, China and Singapore. We also rely on major logistics hubs, primarily in Asia to manufacture and distribute our products, and primarily in the southwestern United States to import products into the Americas region. Our operations could be adversely affected if manufacturing, logistics or other operations in these locations are disrupted for any reason, including natural disasters, IT system failures, military actions or economic, business, labor, environmental, public health, regulatory or political issues. The ultimate impact on us, our significant suppliers and our general infrastructure of being located near vulnerable locations is continuing to be assessed .

Our uneven sales cycle makes planning and inventory management difficult and future financial results less predictable.

In some of our businesses, our quarterly sales have periodically reflected a pattern in which a disproportionate percentage of each quarter's total sales occurs towards the end of the quarter. This uneven sales pattern makes predicting revenue, earnings, cash flow from operations and working capital for each financial period difficult, increases the risk of unanticipated variations in our quarterly results and financial condition and places pressure on our inventory management and logistics systems. If predicted demand is substantially greater than orders, there may be excess inventory. Alternatively, if orders substantially exceed predicted demand, we may not be able to fulfill all of the orders received in each quarter and such orders may be canceled. Depending on when they occur in a quarter, developments such as a systems failure, component pricing movements, component shortages or global logistics disruptions, could adversely impact our inventory levels and results of operations in a manner that is disproportionate to the number of days in the quarter affected.

We experience some seasonal trends in the sale of our products that also may produce variations in our quarterly results and financial condition. For example, sales to governments (particularly sales to the U.S. government) are often stronger in the third calendar quarter, and many customers whose fiscal year is the calendar year spend their remaining capital budget authorizations in the fourth calendar quarter prior to new budget constraints in the first calendar quarter of the following year. European sales are often weaker during the summer months. Typically, our third fiscal quarter is our weakest and our fourth fiscal quarter is our strongest. Many of the factors that create and affect seasonal trends are beyond our control.

Changes in U.S. trade policy, including the imposition of tariffs and the resulting consequences, may have a material adverse impact on our business and results of operations.

The U.S. government has adopted a new approach to trade policy and in some cases to renegotiate, or potentially terminate, certain existing bilateral or multi-lateral trade agreements. It has also imposed tariffs on certain foreign goods, including information and communication technology products. These measures may materially increase costs for goods imported into the United States. This in turn could require us to materially increase prices to our customers which may reduce demand, or, if we are unable to increase prices, result in lowering our margin on products sold. Changes in U.S. Trade policy have resulted in, and could result in more, U.S. trading partners adopting responsive trade policy making it more difficult or costly for us to export our products to those countries.

Any failure by us to identify, manage and complete acquisitions, divestitures and other significant transactions successfully could harm our financial results, business and prospects.

As part of our business strategy, we may acquire companies or businesses, divest businesses or assets, enter into strategic alliances and joint ventures and make investments to further our business (collectively, "business combination and investment transactions"). For example, in April 2017, we acquired Nimble Storage, Inc., which provides predictive all-flash and hybrid-flash storage solutions. In May 2016, we completed the sale to Tsinghua Holdings Co., Ltd. ("Tsinghua"), the asset management arm of Tsinghua University in China, of a 51% interest in our wholly owned subsidiary that owns and operates H3C Technologies and our China-based server, storage and technology services businesses for approximately $2.6 billion. On April 1, 2017 and September 1, 2017, we spun off our Enterprise Services and Software businesses, respectively. See also the risk factors below under the heading “Risks Related to the Separations of our Former Enterprise Services Business and our Former Software Segment”.

Risks associated with business combination and investment transactions include the following, any of which could adversely affect our revenue, gross margin, profitability and financial results:

ITEM 1B. Unresolved Staff Comments.

None.

ITEM 2. Properties.

As of October 31, 2018 , we owned or leased approximately 18 million square feet of space worldwide. A summary of the Company's operationally utilized space is provided below.

	As of October 31, 2018		
	Owned	Leased	Total
	(Square feet in millions)		
Administration and support	4.3	6.9	11.2
(Percentage)	38%	62%	100%
Core data centers, manufacturing plants, research and development facilities, and warehouse operations	1.0	1.4	2.4
(Percentage)	42%	58%	100%
Total	5.3	8.3	13.6
(Percentage)	39%	61%	100%

We believe that our existing properties are in good condition and are suitable for the conduct of our business. Substantially all of our properties are utilized in whole or in part by our Hybrid IT and Intelligent Edge segments.

In connection with the HPE Next initiative, we continue to anticipate changes in our real estate portfolio over the next two years. These changes may include reductions in overall space, and an increase in leased space as a percentage of total space.

Principal Executive Offices

Our principal executive offices, including our global headquarters, are located at 3000 Hanover Street, Palo Alto, California, 94304, United States of America ("U.S."). Our principal executive offices, including our global headquarters is expected to be relocated to a facility at 6280 America Center Drive, San Jose, California, 95002, U.S. and this move is expected to be completed by early fiscal 2019.

Product Development, Services and Manufacturing

The locations of our major product development, manufacturing, and Hewlett Packard Labs facilities are as follows:

Americas

Brazil— Campinas
Puerto Rico —Aguadilla

United States —Alpharetta, Andover, Austin, Carrollton, Chippewa Falls, Colorado Springs, Fremont, Fort Collins, Houston, Milpitas, Palo Alto, Roseville, San Jose, Santa Clara, Sunnyvale

Europe, Middle East, Africa

United Kingdom —Bristol, Erskine

Asia Pacific

China —Beijing, Shanghai
India —Bangalore
Japan —Tokyo
Singapore— Singapore
Taiwan— Taipei

ITEM 3. Legal Proceedings.

Information with respect to this item may be found in Note 18, "Litigation and Contingencies", to the Consolidated Financial Statements in Item 8 of Part II, which is incorporated herein by reference.

full potential and derive business insights. Key solutions include HPE 3PAR Storage and HPE Nimble Storage all-flash arrays for mission critical workloads and general purpose workloads, respectively, and big data solutions running on HPE Apollo Servers. Storage also provides comprehensive data protection with HPE StoreOnce and HPE Recovery Manager Central, solutions for secondary workloads and traditional tape, storage networking and disk products, such as HPE MSA and HPE XP.

- *DC Networking* offerings include top-of-rack switches, core switches, and open networking switches. The Company offers a full stack of networking solutions that deliver open, scalable, secure and agile solutions, by enabling programmable fabric, network virtualization, and network management products.

- HPE Pointnext creates preferred IT experiences that power the digital business. The HPE Pointnext team and the Company's extensive partner network provide value across the IT life cycle delivering advice, transformation projects, professional services, support services and operational services for Hybrid IT and the Intelligent Edge. HPE Pointnext is also a provider of on-premises flexible consumption models, such as HPE GreenLake, that enable IT agility, simplify operations and align cost to business value. HPE Pointnext offerings includes Operational services, Advisory and Professional Services, and Communication and Media Solutions ("CMS").

The *Intelligent Edge* business is comprised of enterprise networking and security solutions for businesses of any size, offering secure connectivity for campus and branch environments, operating under the Aruba brand. The primary business drivers for Intelligent Edge solutions are mobility and the Internet of Things ("IoT").

- *HPE Aruba Product* includes wired and wireless local area network hardware products such as Wi-Fi access points, switches, routers, sensors, and software products that include network management, network access control, analytics and assurance, and location services software .
- *HPE Aruba Services* offers professional and support services for the Intelligent Edge portfolio of products.

Financial Services provides flexible investment solutions, such as leasing, financing, IT consumption, and utility programs and asset management services, for customers that facilitate unique technology deployment models and the acquisition of complete IT solutions, including hardware, software and services from Hewlett Packard Enterprise and others. In order to provide flexible services and capabilities that support the entire IT life cycle, FS partners with customers globally to help build investment strategies that enhance their business agility and support their business transformation. FS offers a wide selection of investment solution capabilities for large enterprise customers and channel partners, along with an array of financial options to SMBs and educational and governmental entities.

Corporate Investments includes Hewlett Packard Labs and certain business incubation projects.

Segment Policy

Hewlett Packard Enterprise derives the results of its business segments directly from its internal management reporting system. The accounting policies that Hewlett Packard Enterprise uses to derive segment results are substantially the same as those the consolidated company uses. The CODM measures the performance of each segment based on several metrics, including earnings from operations. The CODM uses these results, in part, to evaluate the performance of, and to allocate resources to each of the segments.

Segment revenue includes revenues from sales to external customers and intersegment revenues that reflect transactions between the segments on an arm's-length basis. Intersegment revenues primarily consist of sales of hardware and software that are sourced internally and, in the majority of the cases, are financed as operating leases by FS to our customers. Hewlett Packard Enterprise's consolidated net revenue is derived and reported after the elimination of intersegment revenues from such arrangements.

Hewlett Packard Enterprise periodically engages in intercompany advanced royalty payment and licensing arrangements that may result in advance payments between subsidiaries. Revenues from these intercompany arrangements are deferred and recognized as earned over the term of the arrangement by the Hewlett Packard Enterprise legal entities involved in such transactions; however, these advanced payments are eliminated from revenues as reported by Hewlett Packard Enterprise and its business segments. As disclosed in Note 8, "Taxes on Earnings", Hewlett Packard Enterprise executed intercompany advanced royalty payment arrangements resulting in advanced payments of $63 million and $439 million during fiscal 2018 and 2017, respectively. In these transactions, the payments were received in the U.S. from a foreign consolidated affiliate, with a deferral of intercompany revenues over the term of the arrangements. The impact of these intercompany arrangements is eliminated from both Hewlett Packard Enterprise's consolidated and segment net revenues.

Exhibit 19

"Magic Quadrant for LTE Network Infrastructure"

Magic Quadrant for LTE Network Infrastructure

Published: 25 July 2016 ID: G00277823

Analyst(s): Kosei Takiishi, Jessica Ekholm, Sylvain Fabre, Frank Marsala, Peter Liu

Summary

Long Term Evolution rollouts continue as more than 500 network-based CSPs have rolled out commercial 4G LTE service. Gartner compares the 10 vendors of end-to-end (radio access and core) infrastructure for LTE networks to help CSP CTOs find the right one for their needs.

Market Definition/Description

This Magic Quadrant evaluates vendors of "end-to-end" Long Term Evolution (LTE) infrastructure — the term Gartner uses to denote radio and core network of cellular infrastructure — for communications service providers (CSPs) wanting to deploy LTE technology, whether as an overlay or with partial integration with, and some reuse of, existing network equipment (see Note 1).

The market for LTE network infrastructure products for CSPs is maturing. Products considered in this Magic Quadrant include radio access infrastructure (eNodeBs and small cells) located in base station sites, and core network equipment, which is where switching and radio resource management are handled. The core network equipment for LTE, a 4G technology, includes new elements not found in 2G and 3G networks, such as the Mobility Management Entity, a packet data network gateway and a serving gateway. This report also considers the IP Multimedia Subsystem (IMS) infrastructure and network elements required for the provision of voice over LTE (VoLTE), which are located in the core network. Also considered from last year are the vendors' approaches for LTE network alternative use cases, such as machine-to-machine (M2M).

We forecast that the worldwide market for end-to-end LTE network infrastructure will grow from $20.9 billion in 2016 to $36.6 billion in 2020, to account for 70% of spending on mobile network infrastructure (see "Forecast: Communications Service Provider Operational Technology, Worldwide, 2013-2020, 1Q16 Update"). We expect LTE to remain the fastest-growing segment of the mobile network infrastructure market.

The worldwide market for end-to-end LTE network infrastructure includes 10 vendors that provide both radio access and core network elements for LTE (see Figure 1).

Magic Quadrant

Figure 1. Magic Quadrant for LTE Network Infrastructure

Research image courtesy of Gartner, Inc.

Source: Gartner (July 2016)

Vendor Strengths and Cautions

Cisco

Cisco is a dominant player in the Evolved Packet Core (EPC) segment of LTE, including policy control, and a supplier of centralized self-organizing networks (SONs). Cisco does not have macrocell/microcell products, but the partnership with Ericsson announced in November 2015 could make amends for that. Incremental revenue opportunities of $1 billion or more are expected for each company by 2018, but in terms of the LTE radio access network, Cisco's returns would be small. Regarding LTE small cells, Cisco is leveraging its enterprise channels to market for reselling SpiderCloud Wireless radio products (with, for example, agreements with Vodafone).

STRENGTHS

Cisco is a leader in the EPC segment, and its Virtualized Packet Core also receives major CSPs' interest. It is a leader in Internet Protocol (IP) technology, which is an advantage as EPC is an all-IP network technology.

Of the vendors in this Magic Quadrant, Cisco has one of the highest scores for overall financial viability.

In 2016, Cisco announced to buy Jasper Technologies, which provides an Internet of Things (IoT) platform. This IoT service has a broad geographic reach, and its integration with existing IoT products can push forward Cisco's Internet of Everything (IoE)/IoT vision of collaborating with other ecosystem partners.

CAUTIONS

The perception among some CSPs is that Cisco still remains principally an IT player.

The vision of the partnership between Ericsson and Cisco to create the networks of the future is interesting, but so far, its progress resulting from the alliance is primarily limited to IP networks and solutions.

Cisco's IMS for VoLTE solution relies on partners, and some CSPs have indicated this can increase project management overhead.

Datang Telecom

Datang Telecom Technology & Industry Group manufactures radio and core network equipment with a focus on Time Division-Synchronous Code Division Multiple Access (TD-SCDMA) and Time Division-Long Term Evolution (TD-LTE) segments. It is best-known for its leading role in developing the Chinese TD-SCDMA 3G mobile telecommunications standard.

In the LTE segment, Datang mobile focuses on TD-LTE and the Chinese market. The company offers end-to-end solutions for TD-LTE networks, including core, access and test terminals. It is one of the TD-LTE suppliers selected by all three Chinese operators, and the company continues seeking out international TD-LTE opportunities, especially in emerging markets, such as Africa and Eastern Europe.

STRENGTHS

Datang is an early adopter and specialist in time division duplex (TDD)-related technologies (TD-SCDMA, TD-LTE and TD-LTE-Advanced) for which it holds a large set of patents.

Datang is a state-owned company and has been positioned as a TDD technology pilot. The support from government in both policy and finance allows Datang to continuously invest in LTE-related research and development.

Datang still has a relatively big market share in the TD-SCDMA market, which it can leverage to sell its TD-LTE solutions with upgrading concepts. Its TD-LTE products have been selected by all three Chinese CSPs' TD-LTE networks, albeit in a minor role.

CAUTIONS

Datang lacks visibility in the global LTE infrastructure market and is involved only in TD-LTE, a minor variety of LTE infrastructure.

Datang lacks system integration and deployment experience in LTE, which is one of the key barriers to wider adoption by CSPs.

In addition to Datang's brand being little-known outside China, the company's focus on TDD technology in its home market does not help it increase its visibility abroad, as the bulk of LTE deployments use frequency division duplex (FDD).

Ericsson

Ericsson remains in a strong position globally in the LTE infrastructure market. The company's end-to-end LTE and multistandard offerings for core, radio access network (RAN), IMS/VoLTE and software-defined networking (SDN)/network function virtualization (NFV), and its installed base in wireless CSPs' networks, together with its professional services, put it in a strong position to win business from CSPs. Ericsson is aggressively cooperating with leading CSPs on the next-generation technology (5G) and seems to be in a strong position to establish a continuous relationship with them. Nevertheless, Ericsson faces continued challenges from competitors, and several CSPs perceive it as lacking flexibility, such as regarding features, pricing structure and support.

STRENGTHS

Ericsson has long had a strong focus on mobile networks, and it is one of the leaders in terms of numbers of LTE deals. Ericsson has many 2G, 3G and 4G accounts in all geographies, including the United States — a country in which some of its competitors are less strong or have yet to enter the LTE market. Incumbency in 2G and 3G accounts has proved invaluable for any vendor looking to supply LTE upgrades, and Ericsson's many long-standing relationships with CSPs are a solid advantage in terms of making it one of the "go to" vendors for LTE upgrades.

CSPs' feedback indicated that the hardware quality and software stability of Ericsson's products are excellent, and the company's customers were first to commercially launch 600 Mbps service using Category 11 devices (using FDD LTE) and have tested the world's first commercial deployments of three-carrier TDD-and-FDD carrier aggregation with 256 quadrature amplitude modulation (QAM).

Ericsson is active with ecosystem partners addressing multiple verticals, such as public safety, utilities and connected cars. Ericsson promotes cellular for IoT with NB-IoT and LTE Category M, and its M2M/IoT connectivity platform — the Device Connection Platform (DCP) — is very useful for CSPs to support IoT/M2M devices.

CAUTIONS

While Ericsson's overall financial position is good, the company's recent growth and profitability have been challenged by a difficult macro environment. The company has announced structural changes to address these concerns, which may include layoffs and further cost cuts in the near term. Such changes must be monitored given their potential for disruption.

Several CSPs have noted that Ericsson can lack flexibility — for example, with most CSPs having to align to Ericsson's features, roadmap and delivery priorities, rather than the other way around.

Ericsson and Cisco formed a global business and technology partnership in November 2015. Their vision to create the networks of the future is interesting, but since Ericsson is relatively self-sufficient in terms of products and services, so far its progress from the alliance is primarily limited to IP networks and solutions.

FiberHome

FiberHome Technologies is one of the leading telecommunications equipment providers with a focus on optical communications. It is best-known for supplying the first optical fiber deployment in China and its leading position in China's optical fibers and cables and optical access network market.

FiberHome has been producing cellular radio products since 1997 and has been shipping small cells since 2014. Other than transmission and access, FiberHome also has core network products but is relatively weak compared with other vendors. Its TD-LTE products were in the suppliers' list of all three CSPs in China. To date, it has been awarded a small portion of the China TD-LTE market share, and its activities have been limited in its home market, China.

STRENGTHS

FiberHome is a state-owned company, and its relationship with the government can help it to continue to gain some market share in China's TD-LTE, especially in its base — Hubei Province.

FiberHome's leading position in the Chinese optical fiber market and close relationships with domestic CSPs can be leveraged for further expansion of its local TD-LTE business.

CAUTIONS

FiberHome focuses on TD-LTE technology and plays a relatively minor role, even in the Chinese LTE market. It has a limited product portfolio and a lack of visibility in the global LTE market.

The revenue from TD-LTE is a very small portion of FiberHome's total revenue, which has limited its investment in LTE 5G-related product development, such as the IoT, multiple input/multiple output (MIMO) and SDN/NFV.

Fujitsu

Fujitsu is a Japanese ICT vendor focused on the technology solution business that includes the IoT, cloud, big data and mobile. Fujitsu has a broad portfolio of IT services, but its mobile network infrastructure business is very focused on the Japanese market, and has only LTE commercial agreements with Japanese CSPs. It cooperates with Nokia on the development of Serving GW (S-GW) and Packet Data Network GW (P-GW) on the EPC provided to NTT Docomo.

STRENGTHS

Fujitsu offers the BroadOne LTE eNodeB base station family with a distributed architecture consisting of a remote radio head and a baseband unit and LTE femtocell for indoor/outdoor use and for enterprises. The BroadOne femtocell supports multifrequency bands, and selects automatically the operating frequency depending on actual network. Fujitsu's Femtocell GW can manage and operate data and control signals to reduce the high load on the core network.

A significant share of NTT Docomo's early investment in LTE in Japan went to Fujitsu, and KDDI also started to use its LTE femtocell that can support VoLTE. Thanks to the relationship with leading CSPs, Fujitsu can improve its product quality quickly.

Fujitsu provides not only mobile network infrastructure but also devices, including smartphones, tablets and feature phones. This can help to improve the quality of its mobile infrastructure product.

CAUTIONS

Fujitsu is very Japan-centric; its only two customers for LTE network infrastructure are in Japan. We have seen no evidence of traction or new contracts in international markets.

Fujitsu's LTE infrastructure product portfolio is not as comprehensive as that of the Leaders.

Huawei

Huawei holds a strong position globally in the LTE market, despite having its sales potential limited by political concerns in the United States, Australia and other countries. The company has a comprehensive portfolio, and its common radio access architecture has been widely accepted by CSPs. Huawei's MBB 2020 Strategy is composed of progressive enhancements of cellular technologies culminating in the future 5G standard. The strategy focuses on supporting more 4G subscribers, more video traffic and the IoT. The company has improved its professional and managed service capability with its SmartCare service solution.

STRENGTHS

Huawei has heavy R&D investment for both FDD and TDD technologies, and it is known to work hard to satisfy customers' demands. Huawei is involved in major TD-LTE network deployments in China, Japan and Europe. It has developed a TD-LTE-based trunking system for use in industries other than telecommunications, which could represent a business opportunity for CSPs.

Huawei has a comprehensive product portfolio not limited to LTE, which includes servers, storage, routers and switches. Optical transportation gives the company an advantage in addressing today's convergence and "cloudification" requirements.

Feedback from CSPs shows that Huawei's portfolio offers more scale and breadth than those in many more-specialized competitors, with a roadmap and feature support that are more aggressive than some competitors'.

CAUTIONS

Political resistance in the United States, Australia and other countries to granting Huawei unencumbered market access continues to prevent the company from gaining 4G network share in markets where CSPs would like to buy from it.

The vendor lock-in of competitors' existing Global System for Mobile Communications (GSM), Universal Mobile Telecommunications System (UMTS) and FDD LTE customers is still challenging, especially in advanced countries.

Huawei has grown organically in the telecommunications industry and is inclined to try to do everything by itself. On the other hand, it has become more active in the partnership and collaboration with various stakeholders during the past few years, but to be a leader in the IoT/5G era, Huawei still needs to improve its partnership strategy further and become more open.

NEC

NEC was one of the first vendors to articulate the need for smaller cells in LTE networks — long before this became a marketing trend. It has international aspirations for LTE networks and has won reference customers outside Japan. NEC is also an early adopter to support SDN/NFV on the CSP network infrastructure, and its virtualized Evolved Packet Core (vEPC) solution has been commercialized.

STRENGTHS

NEC has the capability not only as a mobile network equipment vendor to CSPs but also as a system integrator for M2M/IoT applications for users such as enterprises and the public sector. Their internal collaboration can create values such as value-added service (VAS) integration in the small-cell solution and mobile-edge computing (MEC) introduction.

NEC has a solid customer base in its home market in Japan. It supplied its technology — for example, LTE RAN and core network elements — to NTT Docomo. It has good support for advanced features, such as carrier aggregation, Cloud RAN and SDN/NFV.

NEC's microwave radio system "Pasolink" contributes to reliable, high-capacity backhaul for LTE, and it provides an advantage in supporting Cloud RAN architecture that is fundamental for LTE-Advanced (LTE-A) and 5G in the future.

CAUTIONS

NEC has made some progress toward achieving its ambitions for a global LTE presence, but its commercial deals are still limited because of insufficient marketing, brand invisibility, very Japan-centric product management and shortage of local support. CSPs should confirm its country-level support carefully.

NEC's LTE product portfolio is not as wide as those of the Leaders, making it harder to avoid commoditization.

Japanese radio frequency allocation for LTE is quite different from global trends, so NEC needs to refine its RAN offering to overcome vendor lock-in situations in its global business.

Nokia

Nokia is a leader in the LTE mobile network infrastructure market. It had transformed itself into a lean wireless network specialist but completed its acquisition of Alcatel-Lucent in January 2016. Nokia's presence in deployed LTE networks has enabled it to establish a business for its LTE-A solution and also contribute to testing advanced products, such as its AirScale, which is capable of supporting 5G. On the other hand, Nokia must continue to demonstrate that it can maintain its financial discipline and strong execution as it rationalizes and integrates the assets and operations of Alcatel-Lucent.

STRENGTHS

Nokia has a comprehensive, end-to-end LTE solution that includes radio, EPC, SON, voice core network, transport, network management, security products, public safety and professional services.

As a combined entity, the new Nokia now comes first among the leading vendors in terms of the number of LTE contracts signed.

Nokia has strong traction in countries including Brazil, Russia, India, China, Japan and South Korea for wireless network infrastructure, and it benefits from having good 3G and 4G presence and skills. The new Nokia now also benefits from a strong North American presence brought by Alcatel-Lucent's footprint.

CAUTIONS

Nokia is undertaking a complex integration with Alcatel-Lucent that includes eliminating portfolio overlap and reducing overlapping personnel. Although the current management team's track record in making such changes has been good, there is potential for disruption due to these changes, and therefore, they must be monitored.

Feedback from CSPs shows that Nokia's product portfolio and technology roadmap were slightly less aggressive compared with other Leaders.

CSP clients of the previous Alcatel-Lucent and Nokia need to care about existing products' continuity, including hardware maintenance and software updates and migration plans.

Samsung

Samsung is a South Korean network equipment vendor and is a relatively late comer to the business of Third Generation Partnership Project (3GPP)-based cellular technology. Samsung is also an early innovator of new cellular technologies, such as vEPC, small cell and Cloud RAN.

STRENGTHS

Samsung has established a position in large-scale LTE deployments in South Korea, North America and Japan. It also penetrated the Middle East in 2011 and European LTE markets in 2012, after establishing Samsung Networks Europe.

Samsung has participated in some very advanced commercial deployments of technology (including LTE-A and Cloud RAN solutions) with South Korean CSPs, which are the world's most advanced mobile network operators, and has also conducted some early 5G-related demonstrations. The company is focusing extensively on small-cell technologies and products supporting LTE in the unlicensed spectrum. Its aim is to make LTE-Unlicensed (LTE-U)-enabled small cells to be commercially available in 2016.

Samsung is one of the leading smartphone vendors, and the internal collaboration can help to improve its product quality and push forward its business.

CAUTIONS

Samsung's lack of presence in the 2G/3G network infrastructure market globally hampers its ability to expand its share of the LTE network infrastructure market, as CSPs tend to favor incumbent vendors for upgrades. It is observed that Samsung didn't announce many new LTE customer additions by 1Q16.

Despite some good international traction for its LTE base station business, Samsung's core network business has not yet extended in the global market.

Samsung is very aggressive in cooperating with CSPs around 5G testing, but its momentum is not as strong as three Leaders: Ericsson, Huawei and Nokia.

ZTE

ZTE is one of the key players in the LTE mobile infrastructure market. It places strong emphasis on China and other Asia/Pacific markets, and it has made some progress toward becoming a bigger international player, with some good reference cases, such as MTN. The experience that the company gained from LTE projects in China helps it break through into some key new markets, such as Southeast Asia, India and Europe. ZTE recently unveiled its Pre5G initiatives, which include both early commercialization of 5G key technologies and LTE-Advanced Pro and will build the bridge connecting 4G and 5G.

STRENGTHS

ZTE is a leading supplier in the Chinese 3G/4G market and a key player in the global mobile infrastructure market. This provides it with a steady stream of revenue and much network-building experience.

ZTE continues to demonstrate, test and interoperate advanced capabilities with CSPs — for example, massive MIMO and cloud radio — in order to gain mind share and market share. It has become increasingly visible in Asia (for example, in SoftBank's LTE network in Japan and Telkomsel's LTE in Indonesia), Europe, the Middle East, Africa and Latin America. It can also use its fixed-line products and relationships in these markets to help it access CSPs wanting LTE upgrades and to deepen its cooperation with them.

Feedback from CSPs includes praise for ZTE's flexibility and responsiveness specifically during the initial rollout phase. Its recently improved marketing communications could help it gain visibility.

CAUTIONS

Although ZTE is branching out from China as it gains more contracts and a wider footprint in international markets, it still needs to boost its presence and mind share in more countries. ZTE could benefit from hiring more local support engineers with local network knowledge and language skills as it becomes more international.

ZTE still experiences difficulty competing against stronger players for Tier 1 CSP accounts in Western Europe, in addition to political resistance in some countries. The election of the new board of directors and leadership members in April 2016 also resulted from some security challenges. In the future, it needs to focus on compliance much more and improve its global business.

ZTE is aggressively seeking to have a 5G partnership with CSPs, but its momentum is not as strong as the other three Leaders: Ericsson, Huawei and Nokia.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we

have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

FiberHome Technologies

Dropped

Alcatel-Lucent, after the acquisition by Nokia

Inclusion and Exclusion Criteria

Vendors in this Magic Quadrant supply end-to-end LTE network infrastructure equipment to network-based CSPs. End-to-end equipment includes radio access and core network elements.

Products considered in this Magic Quadrant include radio access infrastructure (eNodeBs and small cells), located in base station sites, and core network equipment, which is where switching and radio resource management are handled. The core network equipment for LTE, a 4G technology, includes new elements not found in 2G and 3G networks, such as the Evolved Packet Core (EPC), which includes the Mobility Management Entity, a packet data network gateway and a signaling gateway. This report also considers the IP Multimedia Subsystem (IMS) infrastructure and network elements required for the provision of voice over LTE (VoLTE), which are located in the core network. This year, we also consider the vendors' approaches for LTE network alternative use cases, such as M2M.

Several vendors have made progress in their security, as well as NFV offerings around LTE, and while these capabilities will get more attention over time from CSPs, they have not yet appeared as a critical, deciding factor in LTE infrastructure procurement and vendor management decisions.

All of the vendors featured have reference customers for LTE technology with CSPs. Many are also covered elsewhere in Gartner's mobile network infrastructure research.

Evaluation Criteria

Ability to Execute

Gartner evaluates technology vendors on the quality and efficacy of the processes, systems, methods and procedures that enable their performance to be competitive, efficient and effective, and to benefit revenue, retention and reputation. Ultimately, we judge vendors on their ability to capitalize on their vision and their success in doing so.

The vendors' positions on the Ability to Execute axis were determined by evaluating them against the following criteria:

Product/Service. Goods and services offered by the vendor that compete in the defined market (radio and core network elements for LTE carrier infrastructure, as well as 4G small cells and IMS support). This includes current product and service capabilities, quality, feature sets and skills, whether offered natively or through OEM agreements or partnerships, as defined in the Market Definition/Description section and detailed in subcriteria. Both radio (macro and small cells) and core network equipment (EPC and IMS) are included. Professional services offerings, including system integration skills specifically relating to LTE, are also considered. In addition, potential advantages gained in the LTE market through capabilities in important neighboring segments are taken into account.

Overall Viability (Business Unit, Financial, Strategy and Organization). This criterion includes an assessment of the overall organization's financial health, which underpins the financial and practical success of the relevant LTE business unit, and the likelihood of that business unit continuing to invest in the product, offer the product and advance the state of the art within the organization's portfolio.

Market Responsiveness and Track Record. The vendor's ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customers' needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness, as well as market traction demonstrated through LTE contract wins. In addition, it covers the vendor's ability to adapt and scale activities to work with its own partners as well as crucial third parties (such as regulators, municipalities and civil works contractors) — in other words, to "cast a wide net" while still being able to execute and scale quickly when opportunities turn into actual LTE contracts.

Marketing Execution. The clarity, quality, creativity and efficacy of programs designed to deliver the vendor's message in order to influence the market, promote the vendor's brand and business, increase awareness of its products, and establish a positive identification with its products, brand and organization in the minds of buyers. This mind share can be driven by a combination of publicity, promotion, thought leadership, word of mouth and sales activities. Also considered is the vendor's

ability to market solutions in different regulatory contexts and to adapt to different CSPs' LTE business models.

Customer Experience. Relationships, products, services and programs that enable the vendor's clients to succeed with the products evaluated. Specifically, this includes the ways in which customers receive technical support or account support. It can also include ancillary tools, customer support programs (and the quality thereof), the availability of user groups, and SLAs.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria

Weighting

Product/Service

High

Overall Viability

Medium

Sales Execution/Pricing

No Rating

Market Responsiveness/Track Record

High

Marketing Execution

Medium

Customer Experience

Medium

Operations

No Rating

Source: Gartner (July 2016)

Completeness of Vision

Gartner also evaluates technology vendors on their ability to articulate logical statements about the market's current and future direction, innovation, customer needs, and competitive forces, and on how well these statements correspond to Gartner's position. Ultimately, vendors are rated on their understanding of how market forces can be exploited to create opportunities for CSPs.

We determined the vendors' positions on the Completeness of Vision axis by evaluating them against the following criteria:

Market Understanding. The vendor's ability to understand buyers' needs and to translate them into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance them with their added vision. The ability to see LTE in the wider context of CSPs' overall network transformation strategies is particularly important, though this insight must be reflected directly in the vendor's product roadmap.

Marketing Strategy. We look for a clear, differentiated set of messages, consistently communicated throughout the organization and externalized through a website, advertising, customer programs and positioning statements. We also assess the alignment of the vendor's LTE marketing strategy and its overall LTE portfolio strategy, including regional focus.

Offering (Product) Strategy. A vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature set as they map to current and future requirements. This includes differentiated approaches to the different LTE segments, including traditional carriers, municipalities and utilities.

Vertical Strategy. The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including verticals.

Innovation. Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes. This includes:

Sustained evidence of technological expertise and adoption of latest advanced features

Ability to commit to an individual CSP's network rollout, where economically feasible

New product development milestones and compliance with the roadmap of milestones

Migration path for existing wireless network infrastructure technologies, including upgrade evolution to LTE, LTE-Advanced, LTE-Advanced Pro and 5G

Support for ecosystem partners via interfaces and interoperability

Demonstration of appropriate budget for R&D planning

Geographic Strategy. The vendor's strategy to direct resources, skills and offerings to meet the specific needs of its home markets — typically outside its native geography — either directly or through partners, channels and subsidiaries, as appropriate for those geographies and markets.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	No Rating
Offering (Product) Strategy	Medium
Business Model	No Rating
Vertical Strategy	

High

Innovation

High

Geographic Strategy

Medium

Source: Gartner (July 2016)

Quadrant Descriptions

Leaders

Leaders typically have a significant number of commercial references for the LTE network equipment market. They also have momentum in this area, as exemplified by new contract wins. They have a broad portfolio and, even where they need partners, they are the preferred prime vendors for CSPs. They appear in nearly all CSP procurements and trials of LTE infrastructure as de facto suppliers, and their presence in the Leaders quadrant tends to be fairly stable. These are high-viability technology providers. They are well-positioned with their current product portfolios and likely to continue to deliver leading products. Leaders do not necessarily offer the best solution for every customer requirement, however, and their products may not be "best of breed" in every area. Overall, Leaders provide solutions that offer relatively low risk and can achieve and sustain deployments of high quality.

Challengers

Challengers have strong market execution capabilities and good solutions, but overall their products lack the breadth and depth of those of Leaders. Their solutions do not indicate a clear vision for how the market is evolving and are not as innovative or advanced as those of Leaders.

Visionaries

Visionaries demonstrate a clear understanding of the market and provide key innovative elements that are illustrative of the market's future. They lack the ability to influence a large part of the market, or have not yet fully expanded their sales and support capabilities to achieve global reach, or do not yet have the funding and scale to execute with the capabilities of Leaders. A characteristic of Visionaries is that their positions in the Magic Quadrant may potentially move over time into other quadrants, where they could attain a more stable state. They could, for example, achieve this stability by gaining strength and scale or wider market adoption (presence in multiple geographical markets and recognition), in which case they could enter the Leaders quadrant, or by judiciously specializing in a smaller segment and ceasing activities in others as part of a strategic transformation, in which case they could enter the Niche Players quadrant.

Niche Players

Niche Players tend to offer products that focus on a particular segment of the market (for example, a given country, such as Japan) or a subset of functionality (such as TD-LTE). They also tend to be more specialized with regard to regional coverage and/or technology. This can be an advantage, because CSPs aligned with the focus of Niche Players can find these vendors' offerings very suitable. In some cases, Niche Players have made specific decisions about where and where not to compete, so being a Niche Player does not preclude having a well-defined strategy. They could also prove attractive partners for some of the larger vendors in this market, thanks to their market specialisms or technological strengths.

Context

When shortlisting vendors, CSPs should take into account the many commitments they need to make when deploying LTE infrastructure in terms of capital investment in eNodeBs for radio access, core network elements and backhaul, as well as time, project duration and the impact on network complexity when LTE is added as an overlay. LTE deployments are such complex projects that replacing an underperforming vendor after implementation has begun can be impractical, even if liquidated damages and penalties are included in the terms of the contract.

There are multiple LTE vendors for CSPs to choose from, but they vary greatly in the scale and scope of their offerings. It is, therefore, vital that CSPs look for equipment providers that have a clear and differentiated network value proposition and strategy, and that emphasize their differentiation, functionality and features. They should also expect quality software.

CSPs also need to know that their vendor will maintain an adequate roadmap and enable them to sustain a high-performance network. Vendors therefore need to show evidence of resources, expertise and capital for investment in LTE technology in the longer term. With regard to vendors

seeking business outside their home market, CSPs should look for evidence that these vendors have effective strategies to direct resources to meet the specific needs of their intended international markets.

To gauge how well vendors meet the above requirements, Gartner scores them using a series of criteria that we developed to capture their capabilities when it comes to addressing CSPs' wants and needs for end-to-end LTE infrastructure, as described above. These criteria are summed up in our framework as vendors' Ability to Execute and Completeness of Vision.

Several vendors in the lower half of the Magic Quadrant (Cisco, Fujitsu, NEC and Samsung) are much broader and larger technology conglomerates than those in the top half. The Leaders in the top half therefore naturally have more commitment to this segment, as they expect to generate a significant proportion of their overall revenue from it. This has strategic implications for vendor selection because, for CSPs, LTE is bound to require a long-sales-cycle, long-cost-recovery model, as well as an upgrade path to 5G networks.

Market Overview

As of 2 June 2016, 503 LTE networks in 167 countries have been commercially launched, according to GSA. Most of them deployed LTE using the FDD mode only, but almost 50 CSPs deployed LTE using the TDD mode only, and almost 20 operators deployed using both LTE FDD and TDD modes.

End-user uptake of LTE will depend on several factors, such as the availability of affordable LTE service plans and LTE-enabled devices. The availability and price of LTE-enabled devices will play a key role in LTE uptake. We forecast that by the end of 2016, LTE devices will reach a $75 price point, which will give the LTE market a boost in terms of reaching end-user segments that have so far shied away from LTE services due to the high price of LTE devices. We predict that, by the end of 2020, sales of FDD LTE and TD-LTE mobile phones to end users will reach 1,683,846,000, which is 81.8% of all sales to end users (see "Forecast: Mobile Phones, Worldwide, 2013-2020, 1Q16 Update").

In terms of service pricing, an increasingly competitive market will create downward pressure on service prices, and we predict that during this year, the price difference between a 3G and an LTE service will be less than 3%. A growing number of CSPs will not be charging a premium for LTE access. Revenue potential lies in being able to offer a superior network experience and thus increase brand recognition and retention and prevent churn. Additionally, we expect an LTE user to use more data than a 3G user; thus, there are upsell opportunities for CSPs.

The growth in LTE users is helping boost mobile data traffic, as the enhanced network experience has encouraged more users to use data-hungry apps such as streaming video. In our latest consumer mobile app survey, we asked, "How long at a time do you typically stream video using your provider's cellular network?" We found that 29% streamed 30 minutes or more, and that the average streaming time per session was 19.1 minutes. In addition, we found that 85% of the U.S. respondents used YouTube regularly and 68% watched Netflix regularly on their mobile phones.

Thus the increased availability of LTE networks, with the launch of new service plans offering more bandwidth at a lesser price, as well as the improved integration of video into mobile apps by 2018, will contribute to the tripling of consumption of mobile video by early adopters from 15 minutes per day.

In terms of usage per LTE connection, we expect that a 4G smartphone user will use 5.3GB of data per month in 2018 and in comparison, a 3G smartphone user will use 1.4GB of data per month (see "Forecast: Mobile Data Traffic, Worldwide, 2011-2018" for further information). Thus, by 2018, a 4G smartphone user will use 3.7 times more data per month than a 3G smartphone user. In total, despite only 17% of all mobile connections utilizing 4G networks, we estimate that 46% of all mobile traffic will be generated by 4G connections by 2018.

This Magic Quadrant examines vendors of end-to-end (radio and core) LTE network infrastructure, but Gartner also monitors several vendors that do not yet meet the minimum criteria for inclusion because they do not offer end-to-end LTE network equipment, instead focusing on only the radio network or the core network. For example, Potevio, New Postcom Equipment and Mitsubishi Electric offer only radio products; Brocade announced its first virtualized Evolved Packet Core (vEPC) offering in 2016.

The number of large vendors in the end-to-end LTE network infrastructure market could continue to decline, as happened in the 2G/3G market even before the latest economic downturn. Further consolidation remains possible, because there are still many vendors in the mobile network infrastructure market, some of which face financial problems or lack the scale and reach needed to remain relevant. CSPs should, therefore, generally continue to consider a diverse set of stable vendors to minimize the risk of disruption from acquisitions in, or departures from, this market, while containing supplier management overheads — although some CSPs have chosen to use a single vendor for their entire mobile network. As network complexity increases with multiband, multilayer (2G, 3G, 4G and Wi-Fi, and soon 5G) and heterogeneous networks with macro and small cells, and now carrier aggregation, it becomes increasingly attractive to use a single vendor just to ensure quality of service and accountability.

In the latest large acquisition in this segment, Nokia gained control of Alcatel-Lucent through a successful public exchange offer in January 2016. Ericsson and Cisco announced a global business and technology partnership to create the networks of the future in November 2015. Vendor alliances and consolidations aim to increase economies of scale and operational efficiency and improve financial standing; however, technology evolution could happen increasingly fast, with new disruptive technologies, such as SDN/NFV, which could allow alternative vendors, such as HP and Intel to come into the LTE infrastructure market.

The race to win business in the LTE infrastructure market is far from over, and vendors are achieving different degrees of traction when it comes to securing commercial contracts with CSPs. CSPs evaluating vendors for selection should consider whether they have a history of high-quality delivery. They should also favor vendors with a strong track record that effectively promotes their LTE network equipment brand and provides clear differentiation beyond standards. CSPs should partner with vendors that show vision and understand their wants and needs. They should choose a vendor not just for its "boxes," but also for long-term service and support, and ultimately also as a partner to help them with their business models for LTE and succeeding technologies.

Most CSPs plan to integrate small cells into their LTE architecture. The more mature LTE networks are already using small cells in their networks, and the number of small cells is increasing rapidly. Small cells are used in a variety of situations: to increase capacity at busy outdoor locations, to provide coverage and capacity at large indoor locations, to provide services within large, medium and small enterprises, to provide femtocell coverage within households and branch offices, and to provide coverage to rural communities and remote locations. Different situations require a different mix of equipment attributes from LTE equipment vendors, and a specific deployment scenario might favor a given vendor over others; but feedback from CSPs is that even with the Leaders, different markets and deployment scenarios dictate using more than one vendor's 4G RAN.

Evidence

Questionnaires sent to and completed by vendors provided Gartner with an up-to-date view of their activities and achievements in relation to LTE.

We held direct discussions with technical personnel from CSPs that have deployed LTE infrastructure from one or more of the vendors profiled.

We also conducted surveys investigating all available and relevant commercial contracts for LTE involving the vendors concerned.

Local Gartner analysts provided country- and region-specific views, as appropriate.

We also requested that vendors provide supplementary information to use in our research.

Our analysis also reflects earlier briefings and credible sources, including publicly available information.

Note 1

Long Term Evolution

"LTE" was initially intended as an acronym to identify the new radio access network introduced in Release 8 of the 3GPP's standards. Its application has since been extended to the entire technology, including core network elements. In this Magic Quadrant, LTE includes not only LTE of 3GPP Release 8 but also LTE-Advanced of 3GPP Release 10 and LTE-Advanced Pro of 3GPP Release 13.

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

Exhibit 20

Excerpts from Lenovo Group Ltd.'s 2017/18 Annual Report

Lenovo Group Limited | 2017/18 Annual Report

Stock Code 992

ABOUT LENOVO

Lenovo (HKSE: 992) (ADR: LNVGY) is a US$45 billion Fortune 500 company with a vision to become the global leader in Intelligent Transformation through smart devices and infrastructure that create the best user experience. Lenovo manufactures one of the world's widest portfolio of connected products, including smartphones (Motorola), tablets, PCs (Thinkpad, Yoga, Lenovo Legion) and workstations as well as AR/VR devices and smart home/office solutions. Lenovo's next generation data center solutions (ThinkSystem, ThinkAgile) are creating the capacity and computing power for the connections that are changing business and society. Lenovo works to inspire the different in everyone and build a smarter future where everyone thrives. Follow us on LinkedIn, Facebook, Twitter, Instagram, Weibo, or visit us at http://www.lenovo.com.

Other non-operating expenses (net) for the years ended March 31, 2018 and 2017 comprise:

For the year ended March 31	2018 US$'000	2017 US$'000
Finance income	**32,145**	27,795
Finance costs	**(263,160)**	(231,627)
Share of (losses)/profits of associates and joint ventures	**(2,506)**	21,411
	(233,521)	(182,421)

Finance income mainly represents interest on bank deposits.

Finance costs for the year increased by 14 percent as compared with last year. This is mainly attributable to the interest expense of US$20 million in relation to the 5-Year US$500 million notes, issued in March 2017, bearing annual interest at 3.875%, and the increase in factoring cost of US$43 million, partly offset by the decrease in interest on promissory note issued to Google Inc. of US$41 million.

Share of (losses)/profits of associates and joint ventures represents operating (losses)/profits arising from principal business activities of respective associates and joint ventures.

FINANCIAL POSITION

The Group's major balance sheet items are set out below:

Non-current assets	2018 US$'000	2017 US$'000
Property, plant and equipment	**1,304,751**	1,236,250
Prepaid lease payments	**507,628**	473,090
Construction-in-progress	**382,845**	413,160
Intangible assets	**8,514,504**	8,349,145
Interests in associates and joint ventures	**35,666**	32,567
Deferred income tax assets	**1,530,623**	1,435,256
Available-for-sale financial assets	**373,077**	255,898
Other non-current assets	**181,759**	122,221
	12,830,853	12,317,587

37 PRINCIPAL SUBSIDIARIES *(continued)*

Company name	Place of incorporation/ establishment	Issued and fully paid up capital	Percentage of issued capital held		Principal activities
			2018	2017	
Lenovo Tecnologia (Brasil) Ltda	Brazil	BRL4,424,321,818	**100%**	100%	Manufacturing and distribution of IT products
Lenovo (Thailand) Limited	Thailand	THB243,000,000	**100%**	100%	Distribution of IT products as well as mobile phone, smart phone and tablet, server and storage
Lenovo (United States) Inc.	United States	US$1	**100%**	100%	Distribution of IT products
Lenovo (Venezuela), SA	Venezuela	VEB3,846,897	**100%**	100%	Distribution of IT products
聯想(西安)有限公司 (Lenovo (Xian) Limited)[1] (Chinese-foreign equity joint venture)	Chinese Mainland	RMB10,000,000	**100%**	100%	Provision of IT services and distribution of IT products
LLC "Lenovo (East Europe/Asia)"	Russia	RUB1,910,000	**100%**	100%	Distribution and marketing of IT products
Medion AG	Germany	EUR48,418,400	**79.83%**	79.83%	Retail and service business for consumer electronic products
Motorola Mobility Comércio de Produtos Eletronicos Ltda.	Brazil	BRL756,663,401	**100%**	100%	Developer, owner, licensor and seller of communications hardware and software
Motorola Mobility International Sales LLC	United States	-	**100%**	100%	Holding company

37 PRINCIPAL SUBSIDIARIES *(continued)*

Company name	Place of incorporation/ establishment	Issued and fully paid up capital	Percentage of issued capital held		Principal activities
			2018	2017	
Motorola Mobility LLC	United States	-	**100%**	100%	Developer, owner, licensor and seller of communications hardware and software
NEC Personal Computers, Ltd.	Japan	JPY500,000,000	**66.64%**	66.64%	Manufacturing and distribution of IT products
深圳聯想海外控股有限公司 (Shenzhen Lenovo Overseas Holdings Limited)[1] (wholly-foreign owned enterprise)	Chinese Mainland	US$760,822,799.24	**100%**	100%	Investment management
Stoneware, Inc.	United States	US$861,341.25	**100%**	100%	Development and distribution of IT products
陽光雨露信息技術服務(北京)有限公司 (Sunny Information Technology Service, Inc.)[1] (Chinese-foreign equity joint venture)	Chinese Mainland	RMB50,000,000	**100%**	100%	Provision of repair services for computer hardware and software systems

Notes:

(i) All the above subsidiaries operate principally in their respective places of incorporation or establishment.

(ii) All the Chinese Mainland subsidiaries and Motorola's subsidiaries are limited liability companies. They have adopted December 31 as their financial year end date for statutory reporting purposes. For the preparation of the consolidated financial statements, financial statements of these Chinese Mainland subsidiaries and Motorola's subsidiaries for the years ended March 31, 2017 and 2018 have been used.

(iii) Medion AG is a publicly traded German stock corporation listed on the Frankfurt am Main stock exchange. The percentage of issued capital held is equivalent to approximately 86.51% (2017: 86.51%) excluding treasury shares.

(iv) In November 2017, the Company entered into an equity interest transfer and framework agreement in relation to disposal of 100% equity interest in 聯想移動通信軟件(武漢)有限公司 (Lenovo Mobile Communication Software (Wuhan) Limited) to a third party.

(v) The company whose English name ends with a "1" is a direct transliteration of its Chinese registered name.

Exhibit 21

"USA Smartphone Market Share: By Quarter"

Counterpoint

US Smartphone Market Share: By Quarter

FEBRUARY 19, 2019 | IN DATA | BY TEAM COUNTERPOINT

Data on this page is updated every quarter

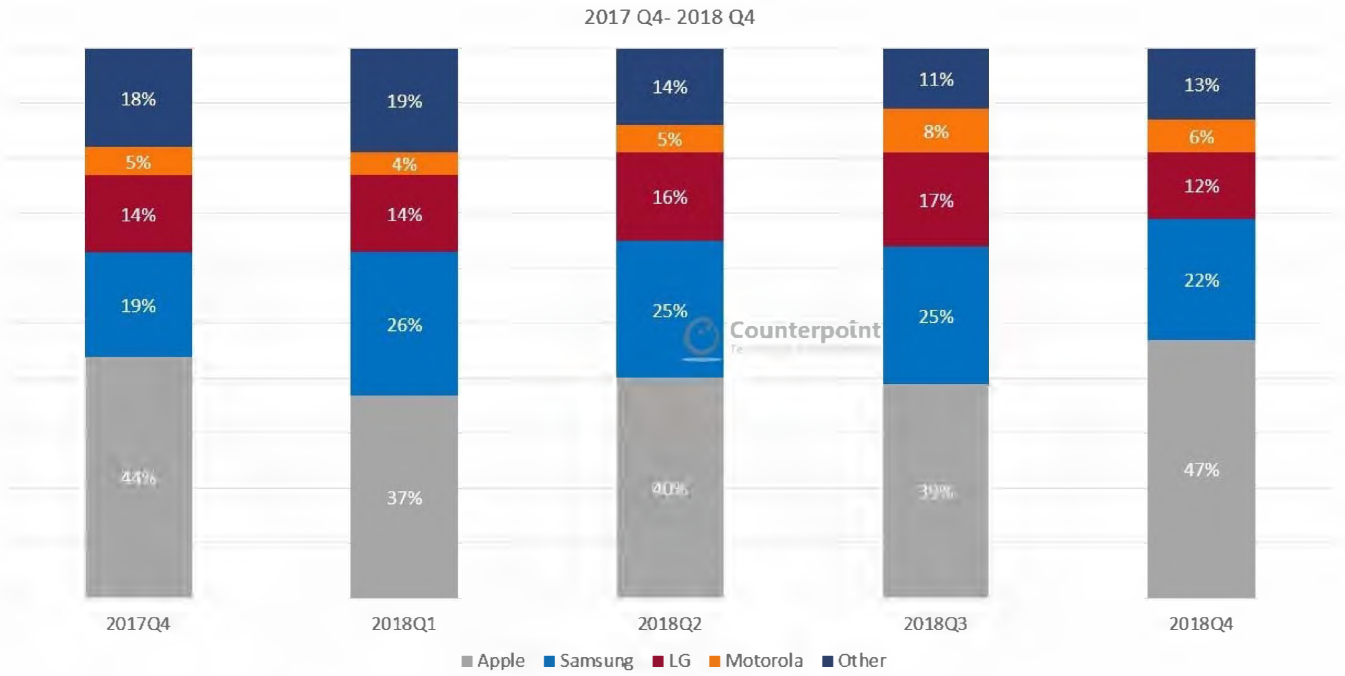
This data represents the US smartphone market share by quarter (from 2016-2018) by top OEMs. The US smartphone market is mainly an operator-driven market.

For detailed insights on the data, please reach out to us at **info(at)counterpointresearch.com**. If you are a member of the press, please contact us at **press(at)counterpointresearch.com** for any media enquiries.

Q4 2018 Highlights

- The US market sold-through 10% fewer smartphones in the fourth quarter of 2018 than the same quarter in 2017.
- Apple: Early adopters hit the stores in September and October to purchase the XS Max and XS. In November and December, the largest volumes moved to the XR.
- Verizon was the largest channel for Apple in 4Q18.
- The only gainers during 4Q18 were Alcatel, Motorola, and Samsung. Alcatel and Motorola grew from small bases.
- Samsung was able to gain on the longevity of the Galaxy S9 and S9 Plus and a particularly strong November for

the Note 9. J7 and J3 variants are strong within many prepaid channels.

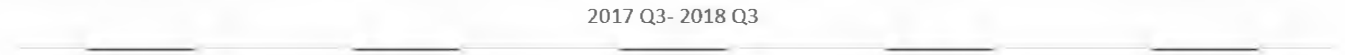


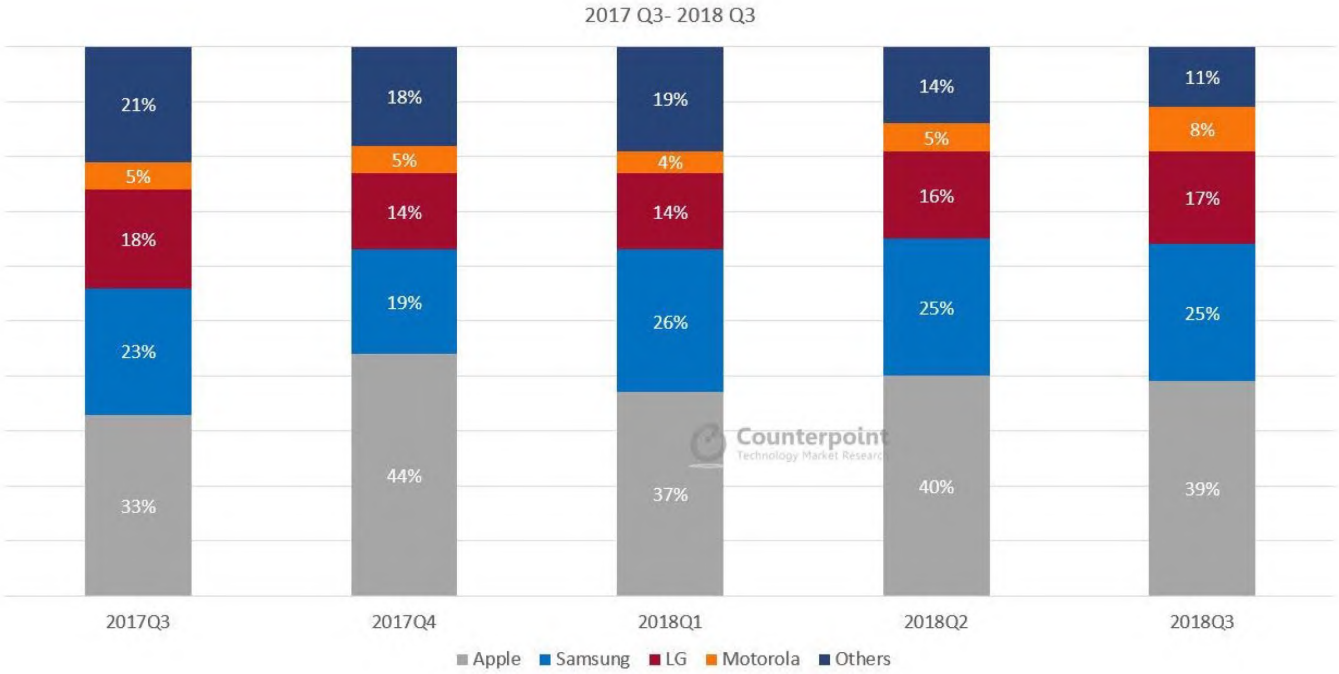
US Smartphone Shipments Market Share (%)	2017Q4	2018Q1	2018Q2	2018Q3	2018Q4
Apple	44%	37%	40%	39%	47%
Samsung	19%	26%	25%	25%	22%
LG	14%	14%	16%	17%	12%
Motorola	5%	4%	5%	8%	6%
Other	18%	19%	14%	11%	13%

Ranking is according to latest quarter.

Q3 2018 Highlights

- The USA smartphone market showed an annual decline of 7%.
- Apple is still leading the US Smartphone market with a 39% share in Q3 2018.
- Motorola showed a YoY growth of 54% in Q3 2018.
- Top four brands contributed to about 90% of the total market share.



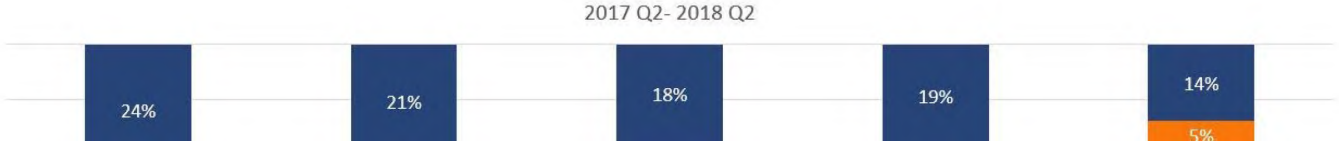


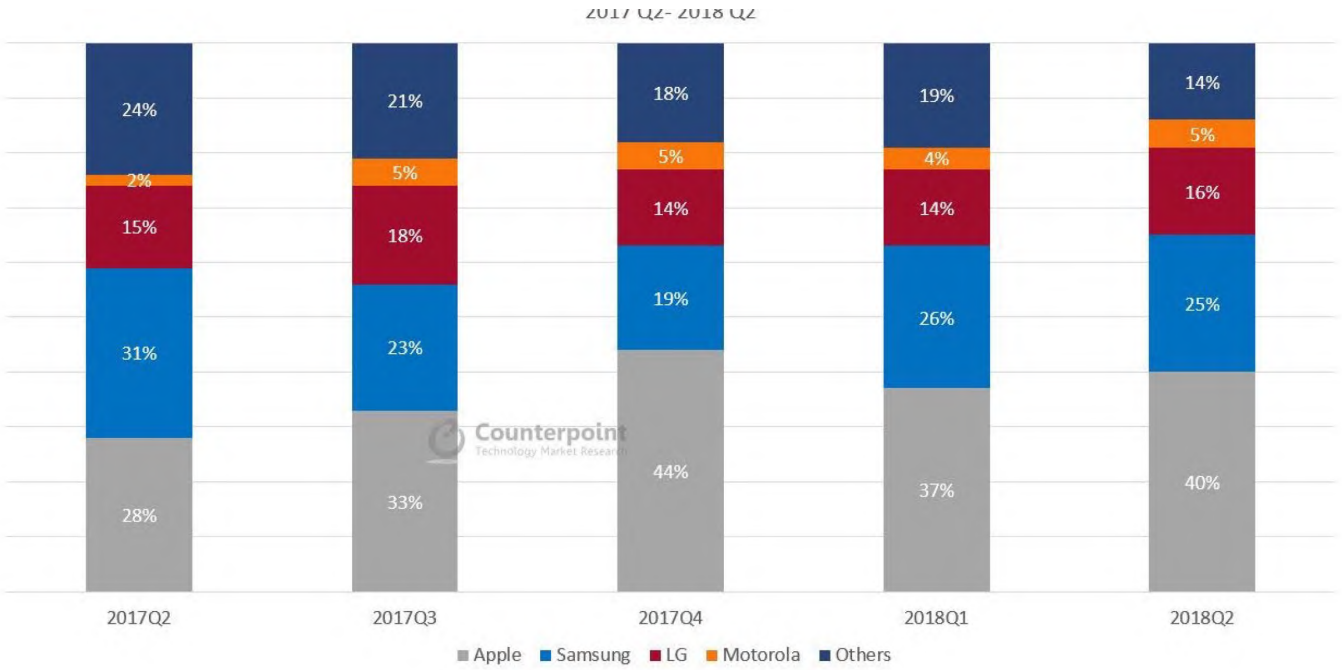
US Smartphone Shipments Market Share (%)	2017Q3	2017Q4	2018Q1	2018Q2	2018Q3
Apple	33%	44%	37%	40%	39%
Samsung	23%	19%	26%	25%	25%
LG	18%	14%	14%	16%	17%
Motorola	5%	5%	4%	5%	8%
Others	21%	18%	19%	14%	11%

Ranking is according to latest quarter.

Q2 2018 Highlights

- The US smartphone market declined 22% annually in Q2 2018.
- The decline in the smartphone market was majorly due to ZTE and Samsung. ZTE was affected due to sanctions imposed by the US government.
- Even though device sales were down by double digits, US wireless performances were solid in Q2 2018.



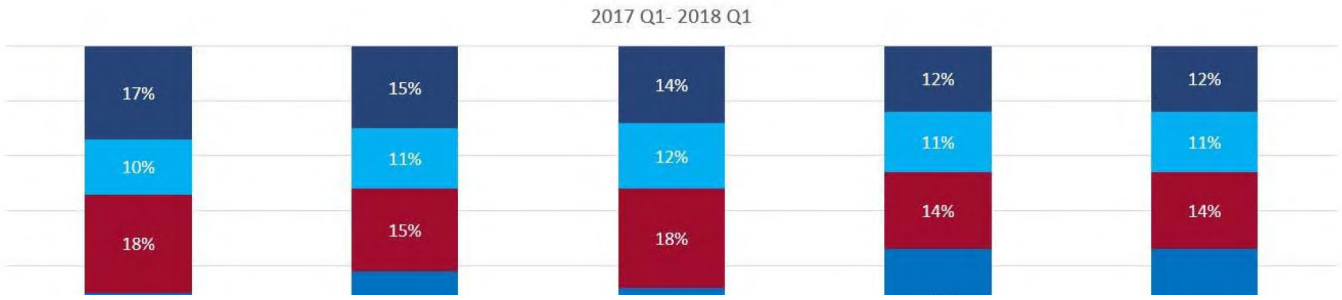


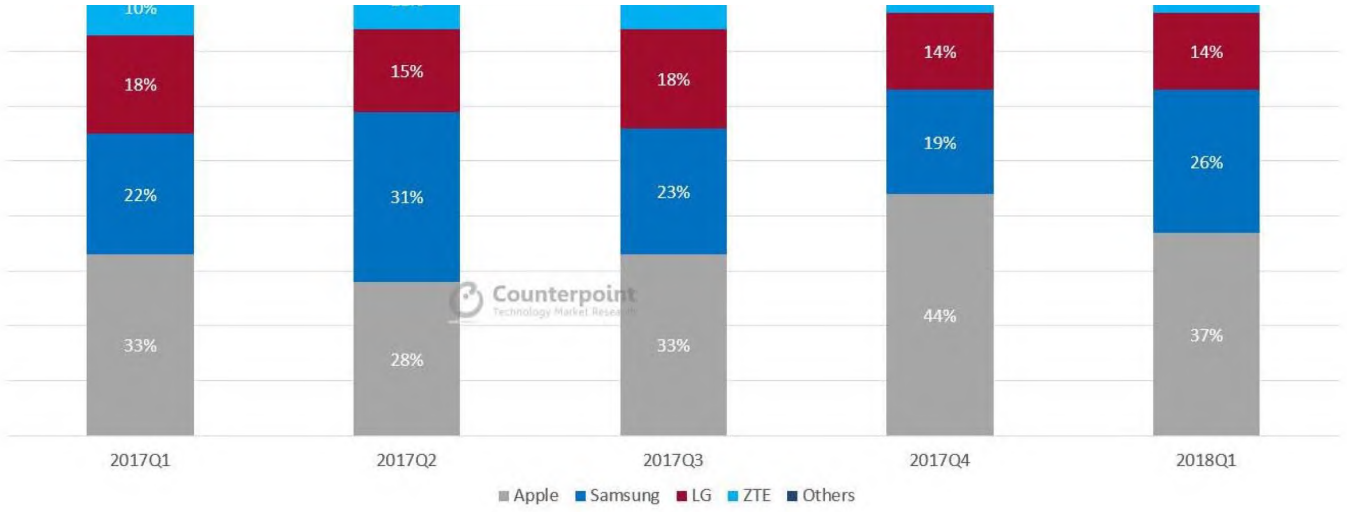
US Smartphone Shipments Market Share (%)	2017Q2	2017Q3	2017Q4	2018Q1	2018Q2
Apple	28%	33%	44%	37%	40%
Samsung	31%	23%	19%	26%	25%
LG	15%	18%	14%	14%	16%
Motorola	2%	5%	5%	4%	5%
Others	24%	21%	18%	19%	14%

Ranking is according to latest quarter.

Q1 2018 Highlights

- The US smartphone market declined by 1% in Q1 2018 compared to Q1 2017
- Apple continued to dominate the smartphone market with 38% share and grew annually because the iPhone X performed well in the market
- LG declined annually due to a shift in its flagship smartphone launch strategy



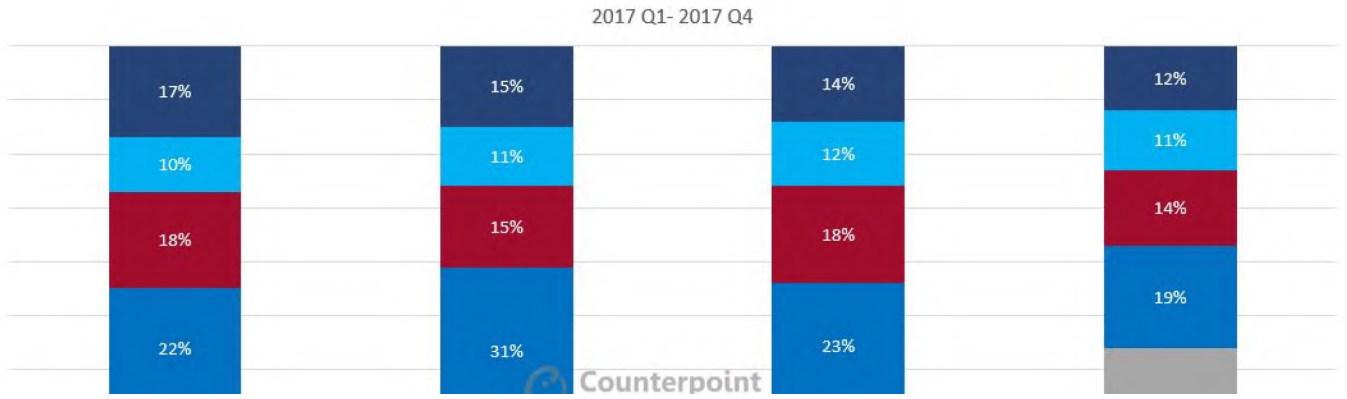


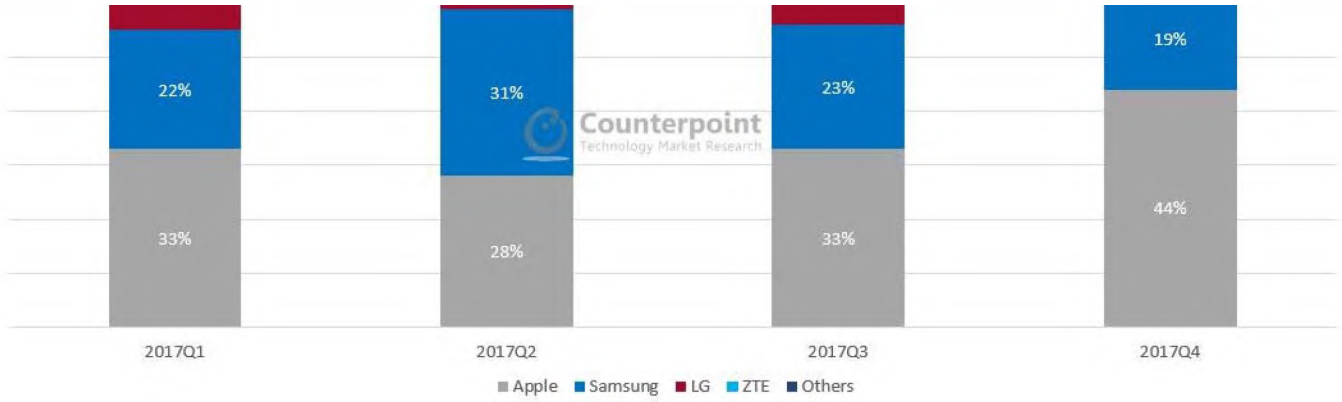
US Smartphone Shipments Market Share (%)	2017Q1	2017Q2	2017Q3	2017Q4	2018Q1
Apple	33%	28%	33%	44%	37%
Samsung	22%	31%	23%	19%	26%
LG	18%	15%	18%	14%	14%
ZTE	10%	11%	12%	11%	11%
Others	17%	15%	14%	12%	12%

Ranking is according to latest quarter.

Q4 2017 Highlights

- US smartphone market witnessed a record holiday quarter shipment, driven mainly by Apple.
- Apple posted a fourth quarter record as well in US, driven by the sales of its latest flagship offerings, iPhone X and iPhone 8 series smartphones.
- Samsung, LG, ZTE and Motorola followed Apple in the top 5 smartphone ranking respectively. Together the top 5 brands captured more than 90% of the total US smartphone market in Q4 2017.





US Smartphone Shipments Market Share (%)	2016 Q1	2016 Q2	2016 Q3	2016 Q4	2017 Q1	2017 Q2	2017 Q3	2017 Q4
Apple	33%	29%	33%	39%	33%	28%	33%	44%
Samsung	28%	30%	25%	19%	22%	31%	23%	19%
LG	14%	14%	13%	13%	18%	15%	18%	14%
ZTE	7%	10%	9%	11%	10%	11%	12%	11%
Others	18%	17%	20%	18%	17%	15%	14%	12%

MARKET SHARE | MARKET SHARE BY QUARTER | SMARTPHONE MARKET SHARE | SMARTPHONES | USA | US SMARTPHONE MARKET SHARE

Team Counterpoint

Counterpoint research is a young and fast growing research firm covering analysis of the tech industry. Coverage areas are connected devices, digital consumer goods, software & applications and other adjacent topics.

for high precision projects.

ALL AUTHOR POSTS

1 Comment counterpointresearch.com 1 Login

Recommend Tweet Share Sort by Best

Join the discussion…

LOG IN WITH OR SIGN UP WITH DISQUS

Name

Bowen Wang • 5 days ago

Where did you get the data

• Reply • Share ›

Subscribe Add Disqus to your siteAdd DisqusAdd Disqus' Privacy PolicyPrivacy PolicyPrivacy

Search...

Your Email

SUBSCRIBE

Exhibit 22

"DoD Issues Cybersecurity Warning Against Lenovo Computers, Handheld Devices"

DOD Issues Cybersecurity Warning Against Lenovo Computers, Handheld Devices

Written by FEDmanager (/component/contact/contact/11?Itemid=101) on 25 October 2016.

The Department of Defense is concerned that computers and handheld devices produced by China-based company Lenovo could be used to spy on Pentagon networks, according to a recent internal study.

The report, produced last month by the J-2 intelligence directorate, also warned that Lenovo is looking to buy American IT firms that would give the company better access to the Pentagon's classified information and introduce compromised hardware into the Defense Department networks, posing cyber espionage risks.

"Although we are concerned any time another nation or individual attempts to initiate intelligence collection against the Department of Defense, we do not discuss internal assessments," said a **Joint Staff spokesman (http://freebeacon.com/national-security/military-warns-chinese-computer-gear-poses-cyber-spy-threat/)**.

The J-2 report also contained a warning that Lenovo was seeking to purchase American information technology companies in a bid to gain access to classified Pentagon and military information networks.

In the past, Lenovo equipment was detected "beaconing," or secretly communicating with remote users during the course of cyber intelligence-gathering, according to one official who added that "There is no way that that company or any Chinese company should be doing business in the United States after all the recent hacking incidents."

According to the Washington Free Beacon, "about 27 percent of Lenovo Group Ltd. is owned by the Chinese Academy of Science, a government research institute. In April, a Chinese Academy of Sciences space imagery expert, Zhou Zhixin, **was named (http://news.ifeng.com/a/20160409/48403966_0.shtml)** to a senior post in the Chinese military's new Strategic Support Force, a unit in charge of space, cyber, and electronic warfare."

A spokesperson with the Pentagon said the Defense Department has not imposed a blanket ban on all Lenovo products, and does not blacklist suppliers or individual products.

The National Security Agency has previously linked China to cyber spying reports against the Pentagon, as well as U.S. and foreign defense contractors, the report stated.

News of the internal study comes days after House Judiciary Chairman Bob Goodlatte **questioned (https://www.politicopro.com/cybersecurity/whiteboard/2016/10/house-chair-questions-clinton-advisers-use-of-chinese-computer-078828)** the FBI for more details about a senior Clinton campaign adviser who used a Lenovo computer to sort her personal from her private emails.

Photo: "Lenovo Laboratory (https://www.flickr.com/photos/fotois/4759074222/in/photolist-8fubzr-8fxsBY-8fxsHu-8fub5D-8fubkp-8fxsnq-8fxsgy-8fubtk-8fxs8o-8fxuXQ-8fud7H-8fucZZ-8fubev-8fudWv-8fud4x-8fxv2U)" by 246-You (https://www.flickr.com/photos/fotois/) is licensed under CC By 2.0 (https://creativecommons.org/licenses/by/2.0/)/ Cropped from original

Posted in General News (/featured/9-general-news)

Tags: cybersecurity (/component/tags/tag/cybersecurity), Federal IT Strategy (/component/tags/tag/federal-it-strategy), DOD (/component/tags/tag/dod), Department of Defense (/component/tags/tag/department-of-defense), Federal IT (/component/tags/tag/federal-it), china (/component/tags/tag/china)

Print

Exhibit 23

Backgrounder, Alcatel-Lucent Enterprise

Backgrounder

Approved for internal and external communication

100 years of innovation, pioneering and setting the course of history

In 2019 ALE celebrates its centenary. For a hundred years ALE and its people have made communication a reality. We invite you to join us on a historical journey which makes ALE the great company it is today.

When we look at our heritage and the 100-year journey, it's easy to see why our people are such pioneers and innovators. It's in the company DNA. It all began in 1919 in the Alsace region when Aaron Weil created a little company called **Le Téléphone Privé** changing the history of telecommunications.

During the 1920s and 30s, the company grew and took the name of **Téléphonie Industrielle et Commerciale** (**Télic**). In 1947, a subsidiary of **Télic** called **Alsatel** (**Société Alsacienne et Lorraine de Télécommunication et d'Electronique**) was created to enable sales expansion. These two companies worked hand in hand. In 1954, **Télic** started to expand with the acquisition of **Cofratel** (**Compagnie Française du Téléphone**). In 1960, **Télic** led the world by delivering the complex Crossbar Telephony technology. Impressed, **CGE** decided to acquire **Télic** under its **Compagnie Industrielle de Téléphone** (**CIT**) division. **CGE** would go on to become a leader in digital communications and would also be known for producing cables, power plants and the TGV high-speed trains in France.

In 1970, a defining moment occurred with the creation of **Alcatel** by merging the **CIT** and **ENTE** (**Énergie Nucléaire Télécommunications et Electronique**), a division of the **Société Alsacienne de Constructions Mécaniques** (**SACM**). **Alcatel** stands for **Alsacienne de Constructions Atomiques, de Télécommunications et d'Electronique**.

In 1980 **Télic**, still a part of **CIT**, changed its name to **Télic-Alcatel**. In the same year **Télic-Alcatel** pioneered and introduced the Minitel, a Videotext online service accessible through telephone lines.

In 1987, a major merger took place between **CGE** and the **ITT** group bringing European centric regions and US and China centric regions together to develop worldwide reach. **Télic-Alcatel's** portfolio merged with the **ITT** group.

In 1991, at parent level, **CGE** became **Alcatel Alsthom**, and at Enterprise level, **Telic-Alcatel** and sister companies (**Bell** and **SEL**) became **Alcatel Business Systems**. The portfolio of voice solutions created at this time lives on in our portfolio of today. In 1991, we proudly launched the first ISDN Videophone with a proprietary VLSI (very large-scale integration) silicon chip, at a time when very few companies were able to design silicon chips.

In 1997, **Alcatel Business Systems** in partnership with **Sun Microsystems** launched the first internet screen phone in Java technology.

One year later, in 1998, the parent company **Alcatel Alsthom** abbreviated its name to **Alcatel** to focus on telecommunications as its core business. An acquisition opportunity arose in 1999 to acquire American companies **Xylan**, **Packet Engines, Assured Access and Internet Devices**, all companies specializing in enterprise network solutions. These companies were merged into the **Alcatel Business Systems** company which would become **Alcatel-Lucent Enterprise** in 2011.

Backgrounder

Approved for internal and external communication

In 2006, the parent company **Alcatel** and **Lucent Technologies** merged to become the modern **Alcatel-Lucent**, a telecommunications giant, today part of **Nokia**. In 2014, via a carve out, **Alcatel-Lucent Enterprise** was acquired by **China Huaxin Post & Telecommunication Economy Development Center**. We have since introduced our Hybrid Cloud Communication solutions, persistent Team Messaging, and the first open CPaaS platform, as well as unified access for wired and wireless networks and intelligent fabric to automate network deployments.

In 2019 our centenary program takes us through this journey and beyond, looking into the future to explore new technologies born from a unique heritage and expertise. We look at what the next 100 years might bring as ALE continues to lead the world in B2B digital transformation, cloud, vertical solutions and the Internet of Things.

Additional information
Word count: 602

Exhibit 24

Alpha Networks, Inc.'s
"Design Manufacturing, Service (DMS)" Webpage

About Alpha

Design , Manufacturing, Service (DMS)

Founded	September, 2003
Headquarter	Hsinchu Science Park, Taiwan
IPO	2004, Taiwan Stock Exchange
Paid-in-Capital	NT$ 5.44 bln (US$ 186 mln)
Number of Employees	More than 3,500
R&D Centers	Hsinchu, Taiwan; Taipei, Taiwan; Chengdu, China; Irvine, U.S.A.
Manufacturing Locations	Hsinchu, Taiwan; Dongguan, China; Changshu, China
Sales Locations	Taiwan, U.S.A., Japan, and China
Business Model	Design、Manufacturing、Service (DMS)

Vision

Forge the Internet to connect people and things.

Mission

Alpha Networks is a globally recognized, professional networking DMS supplier.
We use advanced technology to provide our customers with outstanding solutions at the best value.

Alpha+ Strategy

Alpha Values

Ethics

We value integrity and lead by example.We commit to strict confidentiality and avoid all conflicts of interest.

Customer Values

We put the values and needs of our customers first and commit to deliver.

Agility

We respond swiftly to customer needs and identify market trends to develop the best solutions.

Network Performance

We fully optimize the networking process to generate the optimal outcome.

LAN/MAN

Bare Metal Switch
Data Center Switch
Enterprise Switch
SMB Switch
Metro Ethernet Access Switch
Broadband Access Switch
Industrial Ethernet Switch

WIRELESS BROADBAND

Small Cell
LTE Router
GPON
VDSL IAD
VDSL Router
Wireless Router
WLAN Access Point

DIGITAL MULTIMEDIA

IP Camera
Smart Home

MOBILE ENTERPRISE SOLUTIONS

Intelligent Radar

Company

Capability

Investor Relations

Career

CSR

News

Contact Us

繁 簡

+886-3-563-6666

No.8 Li-shing 7th Rd., Science-based Industrial Park, Hsinchu, Taiwan, R.O.C

GPL Source Code Statement

Exhibit 25

Alpha Networks, Inc.'s "About Alpha" Webpage

ABOUT ALPHA

A Networking DMS Leader with Global Experience

Founded in September 2003, as a spin-off from the D-Link Corporation, Alpha Networks Inc. offers customers nearly 30 years of experience in the networking industry. Alpha possesses highly capable design, manufacturing, and service resources in networking products and offers a complete portfolio of off-the-shelf and custom solutions. Since its inception, Alpha Networks has enjoyed consistent, strong growth and successfully built its reputation by delivering comprehensive product portfolios that deploy a variety of mature and cutting edge technologies. Additionally, by leveraging market intelligence and global experience derived from solid partnerships with first-tier brand name companies, Alpha Networks has proved itself capable of developing design and manufacturing expertise that often push the boundaries of innovation and have helped to elevate Alpha Networks to a position of global leadership in the networking industry.

About Alpha

Our guidance is Integrity, Teamwork, Excellence, Innovation.

Milestones

Milestone timeline of Alpha Networks's success.

Global Presence

Macroscopic Overview with Local Support.

Contact Us

繁 简

+886-3-563-6666

No.8 Li-shing 7th Rd., Science-based Industrial Park, Hsinchu, Taiwan, R.O.C

GPL Source Code Statement

Exhibit 26

Excerpts from Arista Networks, Inc.'s Form 10-K Annual Report for the Fiscal Year 2018

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 10-K

(Mark One)

☒ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the fiscal year ended December 31, 2018

Or

☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the transition period from to

Commission file number: 001-36468

ARISTA NETWORKS, INC.

(Exact name of registrant as specified in its charter)

Delaware	**20-1751121**
(State or other jurisdiction of incorporation or organization)	**(I.R.S. Employer Identification Number)**

5453 Great America Parkway
Santa Clara, California 95054
(Address of principal executive offices)

(408) 547-5500
(Registrant's telephone number, including area code)
Securities registered pursuant to Section 12(b) of the Act:

Title of each class	**Name of each exchange on which registered**
Common Stock, $0.0001 par value	New York Stock Exchange

Securities registered pursuant to Section 12(g) of the Act: None

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ☒ No ☐

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Exchange Act. Yes ☐ No ☒

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T (§232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit such files). Yes ☒ No ☐

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K is not contained herein, and will not be contained, to the best of registrant's knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K. ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, a smaller reporting company, or an emerging growth company. See definitions of "large accelerated filer," "accelerated filer," "smaller reporting company" and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large accelerated filer ☒	Accelerated filer ☐
Non-accelerated filer ☐	Smaller reporting company ☐
	Emerging growth company ☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ☐ No ☒

The aggregate market value of the registrant's common stock held by non-affiliates of the registrant was approximately $14,715,944,627 as of June 30, 2018 b ased on the closing sale price of the registrant's common stock on the New York Stock Exchange on such date. Shares held by persons who may be deemed affiliates have been excluded. This determination of affiliate status is not necessarily a conclusive determination for other purposes.

On February 8, 2019 , 75,730,873 shares of the registrant's common stock were outstanding.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the registrant's definitive Proxy Statement relating to its 2019 Annual Stockholders' Meeting to be filed pursuant to Regulation 14A within 120 days after the registrant's fiscal year end of December 31, 2018 are incorporated by reference into Part III of this Annual Report on Form 10-K.

Our Market Opportunity

We compete primarily in the data center switching market for 10 Gigabit Ethernet and above, excluding blade switches. We also compete in the enterprise campus market for 1 Gigabit Ethernet switching and above and cloud-managed wireless networking.

We believe that cloud computing represents a fundamental shift from traditional legacy data centers and that cloud networking is the fastest growing segment within the data center switching market. As organizations of all sizes are adopting cloud architectures, spending on cloud and next-generation data centers has increased rapidly over the last several years, while traditional legacy IT spending has been growing more slowly. Our 7150, 7050, 7250, 7300 and 7500 Series platforms are now listed on the U. S. Department of Defense Approved Products Lists Integrated Tracking System by the Defense Information Systems Agency.

Our Customers

As of December 31, 2018 , we had delivered our cloud networking solutions to over 5,500 end customers worldwide in approximately 86 countries. Our end customers span a range of industries and include large internet companies, service providers, financial services organizations, government agencies, media and entertainment companies and others. For each of the years ended December 31, 2018 , 2017 , and 2016 , Microsoft purchases, through our channel partner World Wide Technology, Inc., accounted for more than 10% of our total revenue.

Our Competitive Strengths

We believe the following strengths will allow us to maintain and extend our technology leadership position in cloud networking and next-generation data center Ethernet products:

- ***Purpose-Built Cloud Networking Platform.*** We have developed a highly scalable cloud networking platform that uses software to address the needs of large-scale internet companies, cloud service providers, financial services organizations, government agencies and media and entertainment companies, including virtualization, big data and low-latency applications. As a result, our cloud networking platform does not have the inherent limitations of legacy network architectures.
- ***Broad and Differentiated Portfolio.*** Using multiple silicon architectures, we deliver switches and routers with industry-leading capacity, low latency, port density and power efficiency and have innovated in areas such as deep packet buffers, embedded optics and reversible cooling. Our broad portfolio has allowed us to offer customers products that best match their specific requirements.
- ***Single Binary Image Software.*** The single binary image of EOS software allows us to maintain feature consistency across our entire product portfolio and enables us to introduce new software innovations into the market that become available to our entire installed base without a "forklift upgrade" (i.e., a broad upgrade of the data center infrastructure).
- ***Rapid Development of New Features and Applications.*** Our highly modular EOS software has allowed us to rapidly deliver new features and applications while preserving the structural integrity and quality of our network operating system. We believe our ability to deliver new features and capabilities more quickly than legacy switch/router operators, provides us with a strategic advantage given that the requirements in cloud and next-generation data center networking continue to evolve rapidly.
- ***Deep Understanding of Customer Requirements.*** We have developed close working relationships with many of our largest customers that provide us with insights about their needs and future requirements. This has allowed us to develop and deliver products to market that meet customer demands and expectations as well as to rapidly grow sales to existing customers.
- ***Strong Management and Engineering Team with Significant Data Center Networking Expertise.*** Our management and engineering team consists of networking veterans with extensive data center networking expertise. Our President and Chief Executive Officer, Jayshree Ullal, with 30+ years of networking expertise from silicon to systems companies. Andy Bechtolsheim, our Founder and Chief Development Officer, was previously a Founder and chief system architect at Sun Microsystems. Kenneth Duda, our Founder and Chief Technology Officer, led the software development effort of EOS.

- ***Significant Technology Lead.*** We believe that our networking technology represents a fundamental advance in networking software. Our EOS software is state-driven and the result of more than 1,000 man-years of research and development investment over a ten-year period with 10+ million lines of code as a key cloud networking software stack.

Our Products and Technology

We offer one of the broadest product lines of data center 10/25/40/50/100 Gigabit Ethernet switches and routers in the industry, comprising our 7010/7020 Series, 7050X Series, 7060X Series, 7130 Series, 7160 Series, 7150 Series, 7170 Series, 7250X Series, 7260 Series, 7280R Series Universal Leaf products, 7300X Series Spline products, and our 7500R Series Universal Spine products.

We deliver routing and switching platforms with industry-leading capacity, low latency, port density and power efficiency. We have also innovated in areas such as deep packet buffers, embedded optics and reversible cooling. An overview of our switching/routing portfolio is shown in the figure below.

We use multiple silicon architectures across our products, which allows us to build a broader range of products optimized for different functions in the network than competitors that utilize fewer silicon architectures. While we use multiple silicon architectures, all of our platforms are powered with the same binary EOS image, which significantly simplifies deployment and ensures the same rich feature set and consistent operation across all our products.

Our Extensible Operating System

The core of our cloud networking platform is our Extensible Operating System, or EOS, which runs on top of standard Linux and offers programmability at all layers of the stack. All of our 10/25/40/50/100 Gigabit Ethernet platforms run our EOS software.

EOS is based on a new and innovative architecture that is highly modular and consists of more than 100 separate processes that we call agents, each one handling specific protocol processing, device driver or system management functions. Each agent runs in user space as a separate Linux process and is completely protected and isolated from all other agents.

We are constantly investing in our core infrastructure to provide the capabilities required for building modern cloud networks and enhancing scalability. New requirements for use in cloud and service provider networks and hybrid cloud deployments in enterprises require on-going upgrades and extensions to our state oriented architecture.

EOS Attributes

The modular and programmable architecture of EOS enables us to offer a set of attributes, capabilities and features that are essential for cloud networking and next-generation data centers.

- greater risk of unexpected changes in regulatory practices, tariffs and tax laws and treaties, including the Tax Act;
- greater risk of unexpected changes in tariffs imposed by the U.S. on goods from other countries and tariffs imposed by other countries on U.S. goods, including the tariffs recently implemented and additional tariffs that have been proposed by the U.S. government on various imports from China, Canada, Mexico and the EU, and by the governments of these jurisdictions on certain U.S. goods, and any other possible tariffs that may be imposed on services such as ours, the scope and duration of which, if implemented, remain uncertain;
- deterioration of political relations between the U.S. and Canada, the U.K., the EU and China, which could have a material adverse effect on our sales and operations in these countries;
- greater risk of changes in diplomatic and trade relationships, including new tariffs, trade protection measures, import or export licensing requirements, trade embargoes and other trade barriers;
- the uncertainty of protection for intellectual property rights in some countries;
- greater risk of a failure of foreign employees to comply with both U.S. and foreign laws, including antitrust regulations, the FCPA and any trade regulations ensuring fair trade practices; and
- heightened risk of unfair or corrupt business practices in certain geographies and of improper or fraudulent sales arrangements that may impact financial results and result in restatements of, or irregularities in, financial statements.

These and other factors could harm our ability to gain future international revenue and, consequently, materially affect our business, financial condition, results of operations and prospects. Expanding our existing international operations and entering into additional international markets will require significant management attention and financial commitments. Our failure to successfully manage our international operations and the associated risks effectively could limit our future growth or materially adversely affect our business, financial condition, results of operations and prospects.

Moreover, our business is also impacted by the negotiation and implementation of free trade agreements between the United States and other countries. Such agreements can reduce barriers to international trade and thus the cost of conducting business overseas. For instance, the United States recently reached a new trilateral trade agreement with the governments of Canada and Mexico to replace the North American Free Trade Agreement ("NAFTA"). If the United States withdraws from NAFTA and the three countries fail to approve the new agreements, known as the United States-Mexico-Canada Agreement, our cost of doing business within the three countries could increase.

The United Kingdom's vote to leave the European Union will have uncertain effects and could adversely affect us.

On June 23, 2016, the electorate in the United Kingdom, or UK, voted in favor of leaving the European Union, or EU, (commonly referred to as the "Brexit"). Thereafter, on March 29, 2017, the country formally notified the EU of its intention to withdraw pursuant to Article 50 of the Lisbon Treaty, triggering the two-year negotiation period for exiting the EU. The withdrawal of the UK from the EU is scheduled to take effect on March 29, 2019 either on the effective date of the withdrawal agreement or, in the absence of agreement, two years after the UK provides a notice of withdrawal pursuant to the EU Treaty and transitional provisions may or may not be put in place to ease the process.

The effects of Brexit will depend on agreements the UK makes to retain access to EU markets either during a transitional period or more permanently. Brexit creates an uncertain political and economic environment in the UK and potentially across other EU member states for the foreseeable future, including during any period while the terms of Brexit are being negotiated and such uncertainties could impair or limit our ability to transact business in the member EU states.

Further, Brexit could adversely affect European and worldwide economic or market conditions and could contribute to instability in global financial markets, and the value of the Pound Sterling currency or other currencies, including the Euro. We are exposed to the economic, market and fiscal conditions in the UK and the EU and to

changes in any of these conditions. Depending on the terms reached regarding Brexit, it is possible that there may be adverse practical and/or operational implications on our business.

A significant amount of the regulatory regime that applies to us in the UK is derived from EU directives and regulations. For so long as the UK remains a member of the EU, those sources of legislation will (unless otherwise repealed or amended) remain in effect. However, Brexit could change the legal and regulatory framework within the UK where we operate and is likely to lead to legal uncertainty and potentially divergent national laws and regulations as the UK determines which EU laws to replace or replicate. Consequently, no assurance can be given as to the impact of Brexit and, in particular, no assurance can be given that our operating results, financial condition and prospects would not be adversely impacted by the result.

Enhanced United States tax, tariff, import/export restrictions, Chinese regulations or other trade barriers may have a negative effect on global economic conditions, financial markets and our business.

There is currently significant uncertainty about the future relationship between the United States and various other countries, most significantly China, with respect trade policies, treaties, tariffs and taxes, including trade policies and tariffs regarding China. The current U.S. Administration has called for substantial changes to U.S. foreign trade policy with respect to China and other countries, including the possibility of imposing greater restrictions on international trade and significant increases in tariffs on goods imported into the United States. In 2018, the Office of the U.S. Trade Representative (the "USTR") enacted tariffs on imports into the U.S. from China, including communications equipment products and components manufactured and imported from China. The tariff became effective on September 24, 2018, with an initial rate of 10% and was scheduled to increase from 10% to 25% on January 1, 2019; however, that increase has been delayed for 90 days pending trade negotiations between the U.S. and China. In addition, the tariffs may be increased in the future. It is expected that these tariffs will cause our costs to increase, which could narrow the profits we earn from sales of products requiring such materials. Furthermore, if tariffs, trade restrictions, or trade barriers are placed on products such as ours by foreign governments, especially China, the prices for our products may increase, which may result in the loss of customers and our business, financial condition and results of operations may be harmed. We believe we can adjust our supply chain and manufacturing practices to minimize the impact of the tariffs, but our efforts may not be successful, there can be no assurance that we will not experience a disruption in our business related to these or other changes in trade practices and the process of changing suppliers in order to mitigate any such tariff costs could be complicated, time-consuming, and costly.

Furthermore, the U.S. tariffs may cause customers to delay orders as they evaluate where to take delivery of our products in connection with their efforts to mitigate their own tariff exposure. Such delays create forecasting difficulties for us and increase the risk that orders might be canceled or might never be placed. Current or future tariffs imposed by the U.S. may also negatively impact our customers' sales, thereby causing an indirect negative impact on our own sales. Any reduction in our customers' sales, and/or any apprehension among distributors and customers of a possible reduction in such sales, would likely cause an indirect negative impact on our own sales. Even in the absence of further tariffs, the related uncertainty and the market's fear of an escalating trade war might cause our distributors and customers to place fewer orders for our products, which could have a material adverse effect on our business, liquidity, financial condition, and/or results of operations.

Additionally, the current U.S. Administration continues to signal that it may alter trade agreements and terms between China and the United States, including limiting trade with China, and may impose additional tariffs on imports from China. Therefore, it is possible further tariffs may be imposed that could cover imports of communications equipment products and components used in our products, or our business may be adversely impacted by retaliatory trade measures taken by China or other countries, including restricted access to suppliers, communications equipment products and components used in our products, causing us to raise prices or make changes to our products, which could materially harm our business, financial condition and results of operations. The current administration, along with Congress, has created significant uncertainty about the future relationship between the United States and other countries with respect to the trade policies, treaties, taxes, government regulations and tariffs that would be applicable. It is unclear what changes might be considered or implemented and what response to any such changes may be by the governments of other countries. These changes have created significant uncertainty about the future relationship between the United States and China, as well as other countries, including with respect to the trade policies, treaties, government regulations and tariffs that could apply to trade

- obsolescence charges;
- changes in shipment volume;
- the timing of revenue recognition and revenue deferrals;
- increased cost, loss of cost savings or dilution of savings due to changes in component pricing or charges incurred due to inventory holding periods if parts ordering does not correctly anticipate product demand or if the financial health of either contract manufacturers or suppliers deteriorates;
- increased costs arising from the tariffs imposed by the U.S. on goods from other countries and tariffs imposed by other countries on U.S. goods, including the tariffs recently implemented and additional tariffs that have been proposed by the U.S. government on various imports from China, Canada, Mexico and the E.U. and by the governments of these jurisdictions on certain U.S. goods;
- lower than expected benefits from value engineering;
- changes in distribution channels;
- increased warranty costs; and
- our ability to execute our strategy and operating plans.

We determine our operating expenses largely on the basis of anticipated revenues and a high percentage of our expenses are fixed in the short and medium term. As a result, a failure or delay in generating or recognizing revenue could cause significant variations in our operating results and operating margin from quarter to quarter. Failure to sustain or improve our gross margins reduces our profitability and may have a material adverse effect on our business and stock price.

Our sales cycles can be long and unpredictable, and our sales efforts require considerable time and expense. As a result, our sales and revenue are difficult to predict and may vary substantially from period to period, which may cause our results of operations to fluctuate significantly.

The timing of our sales and revenue recognition is difficult to predict because of the length and unpredictability of our products' sales cycles. A sales cycle is the period between initial contact with a prospective end customer and any sale of our products. End-customer orders often involve the purchase of multiple products. These orders are complex and difficult to complete because prospective end customers generally consider a number of factors over an extended period of time before committing to purchase the products and solutions we sell. End customers, especially in the case of our large end customers, often view the purchase of our products as a significant and strategic decision and require considerable time to evaluate, test and qualify our products prior to making a purchase decision and placing an order. The length of time that end customers devote to their evaluation, contract negotiation and budgeting processes varies significantly. Our products' sales cycles can be lengthy in certain cases, especially with respect to our prospective large end customers. During the sales cycle, we expend significant time and money on sales and marketing activities and make investments in evaluation equipment, all of which lower our operating margins, particularly if no sale occurs. Even if an end customer decides to purchase our products, there are many factors affecting the timing of our recognition of revenue, which makes our revenue difficult to forecast. For example, there may be unexpected delays in an end customer's internal procurement processes, particularly for some of our larger end customers for which our products represent a very small percentage of their total procurement activity. There are many other factors specific to end customers that contribute to the timing of their purchases and the variability of our revenue recognition, including the strategic importance of a particular project to an end customer, budgetary constraints and changes in their personnel.

Even after an end customer makes a purchase, there may be circumstances or terms relating to the purchase that delay our ability to recognize revenue from that purchase. In addition, the significance and timing of our product enhancements, and the introduction of new products by our competitors, may also affect end customers' purchases. For all of these reasons, it is difficult to predict whether a sale will be completed, the particular period in which a sale will be completed or the period in which revenue from a sale will be recognized. If our sales cycles lengthen, our revenue could be lower than expected, which would have an adverse effect on our business, financial condition, results of operations and prospects.

- a classified board of directors with three-year staggered terms, which could delay the ability of stockholders to change the membership of a majority of our board of directors;
- the ability of our board of directors to issue shares of preferred stock and to determine the price and other terms of those shares, including preferences and voting rights, without stockholder approval, which could be used to significantly dilute the ownership of a hostile acquirer;
- the exclusive right of our board of directors to elect a director to fill a vacancy created by the expansion of our board of directors or the resignation, death or removal of a director, which prevents stockholders from being able to fill vacancies on our board of directors;
- a prohibition on stockholder action by written consent, which forces stockholder action to be taken at an annual or special meeting of our stockholders;
- the requirement that a special meeting of stockholders may be called only by the chairman of our board of directors, our president, our secretary or a majority vote of our board of directors, which could delay the ability of our stockholders to force consideration of a proposal or to take action, including the removal of directors;
- the requirement for the affirmative vote of holders of at least 66 2/3% of the voting power of all of the then outstanding shares of the voting stock, voting together as a single class, to amend the provisions of our amended and restated certificate of incorporation relating to the issuance of preferred stock and management of our business or our amended and restated bylaws, which may inhibit the ability of an acquirer to effect such amendments to facilitate an unsolicited takeover attempt;
- the ability of our board of directors, by majority vote, to amend the bylaws, which may allow our board of directors to take additional actions to prevent an unsolicited takeover and inhibit the ability of an acquirer to amend the bylaws to facilitate an unsolicited takeover attempt; and
- advance notice procedures with which stockholders must comply to nominate candidates to our board of directors or to propose matters to be acted upon at a stockholders' meeting, which may discourage or deter a potential acquirer from conducting a solicitation of proxies to elect the acquirer's own slate of directors or otherwise attempting to obtain control of us.

In addition, as a Delaware corporation, we are subject to Section 203 of the Delaware General Corporation Law. These provisions may prohibit large stockholders, in particular those owning 15% or more of our outstanding voting stock, from merging or combining with us for a certain period of time.

The issuance of additional stock in connection with financings, acquisitions, investments, our stock incentive plans or otherwise will dilute all other stockholders.

Our amended and restated certificate of incorporation authorizes us to issue up to 1,000,000,000 shares of common stock and up to 100,000,000 shares of preferred stock with such rights and preferences as may be determined by our board of directors. Subject to compliance with applicable rules and regulations, we may issue our shares of common stock or securities convertible into our common stock from time to time in connection with a financing, acquisition, investment, our stock incentive plans or otherwise. We may from time to time issue additional shares of common stock at a discount from the then market price of our common stock. Any issuance of stock could result in substantial dilution to our existing stockholders and cause the market price of our common stock to decline.

Item 1B. Unresolved Staff Comments

None.

Item 2. Properties

Our corporate headquarters is located in Santa Clara, California where we currently lease approximately 210,000 square feet of space under a lease agreement that expires in 2023. In addition, we lease office spaces for operations, sales personnel and research and development in locations throughout the U.S. and various international

locations, including Ireland, Canada, India, Australia, the United Kingdom, Korea, Singapore, Japan, Malaysia, China, Mexico, France, Taiwan, and United Arab Emirates. We also lease data centers in the U.S., Ireland and the United Kingdom.

We believe that our current facilities are adequate to meet our current needs. We intend to expand our facilities or add new facilities as we add employees and enter new geographic markets, and we believe that suitable additional or alternative space will be available as needed to accommodate ongoing operations and any such growth. We expect to incur additional expenses in connection with such new or expanded facilities.

Item 3. Legal Proceedings

The information set forth under the "Legal Proceedings" in Note 7. Commitments and Contingencies of the Notes to Consolidated Financial Statements included in Part II, Item 8, of this Annual Report on Form 10-K is incorporated herein by reference.

Item 4. Mine Safety Disclosures

Not applicable.

Exhibit 27

Excerpts from Extreme Networks, Inc.'s Form 10-K Annual Report for the Fiscal Year Ended June 30, 2018

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

Form 10-K

(Mark One)

☒ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the fiscal year ended June 30, 2018

OR

☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the transition period from to .

Commission file number 000-25711

Extreme Networks, Inc.

(Exact name of Registrant as specified in its charter)

Delaware	**77-0430270**
(State or other jurisdiction of incorporation or organization)	**(I.R.S. Employer Identification No.)**
6480 Via del Oro San Jose, California	**95119**
(Address of principal executive offices)	**(Zip Code)**

Registrant's telephone number, including area code: (408) 579-2800

Securities registered pursuant to Section 12(b) of the Act: None
Securities registered pursuant to Section 12(g) of the Act:
Common stock, $0.001 par value

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ☐ No ☒

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act. Yes ☐ No ☒

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K (§229.405 of this chapter) is not contained herein, and will not be contained, to the best of registrant's knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K. ☐

Indicate by check mark whether the registrant has submitted electronically and posted on its corporate Web site, if any, every Interactive Data File required to be submitted and posted pursuant to Rule 405 of Regulation S-T (§229.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit and post such files). Yes ☒ No ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, smaller reporting company, or an emerging growth company. See the definitions of "large accelerated filer," "accelerated filer," "smaller reporting company," and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large Accelerated Filer	☒	Accelerated Filer	☐
Non-Accelerated Filer	☐	Smaller reporting company	☐
Emerging growth company	☐		

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ☐ No ☒

The aggregate market value of voting stock held by non-affiliates of the Registrant was approximately $1.2 billion as of December 31, 2017 the last business day of the Registrant's most recently completed second fiscal quarter, based upon the per share closing price of the Registrant's common stock as reported on The NASDAQ Global Market reported on such date. For purposes of this disclosure, shares of common stock held or controlled by executive officers and directors of the registrant and by persons who hold more than 5% of the outstanding shares of common stock have been treated as shares held by affiliates. This calculation does not reflect a determination that certain persons are affiliates of the Registrant for any other purpose.

118,320,200 shares of the Registrant's Common stock, $.001 par value, were outstanding as of August 24, 2018.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the registrant's definitive proxy statement for the 2018 Annual Meeting of Stockholders to be filed with the Commission pursuant to Regulation 14A not later than 120 days after the end of the fiscal year covered by this Annual Report on Form 10-K are incorporated herein by reference in Part III of this Annual Report on Form 10-K.

- **The Internet of Things.** The Internet of Things is having dramatic effects on network infrastructure in healthcare, education, manufacturing, government and retail as more "smart" devices are entering the networks. These devices pose opportunities as well as threats to the network.
- **Growing usage of the cloud.** Enterprises have migrated increasing numbers of applications and services to either private clouds or public clouds offered by third parties. In either case, the network infrastructure must adapt to this new dynamic environment. Intelligence and automation are key if enterprises are to derive maximum benefit from their cloud deployments. Ethernet speeds, scaling from 10 Gigabits per second ("G") to 100G, provide the infrastructure for both private and public clouds. In addition, there is growing interest in SDN approaches that may include technologies such as OpenFlow, OpenStack, and CloudStack for increased network agility.
- **Vendor consolidation is expected to continue.** Consolidation of vendors within the enterprise network equipment market and between adjacent markets (storage, security, wireless & voice software and applications) continues to gain momentum. We identified this trend in 2013 with our acquisition of Enterasys. Further, we believe customers are demanding more end-to-end, integrated networking solutions. To address this demand, we acquired the WLAN Business of Zebra in October 2016, the Campus Fabric Business from Avaya in July 2017, and the Data Center Business from Brocade in October 2017.

  Our strategy, product portfolio and research and development are closely aligned with what we have identified as the following trends in our industry:

  - **The software segment of the worldwide enterprise network equipment market has continued to evolve and demands for improvements in Network Management will continue.**
    - ➢ *We announced our Extreme Management Console in Fiscal 2017. This innovative software helps IT network administrators to navigate the unprecedented demands caused by the surge of IoT devices and technology.*
  - **Enterprise adoption of the cloud and open-source options are disrupting traditional license and maintenance business models.**
    - ➢ *We announced cloud offerings in April 2016 and enhanced those offerings in 2017. Extreme began participation in the OpenSwitch program in May 2016 and now participates in the StackStorm community with the acquisition from Brocade in November 2017.*
  - **Enterprise adoption of new financing solutions allows for increased flexibility, Limited investment and zero long-term commitments. These offerings are changing the traditional CAPEX model to (OPEX) models using financing purchases over time are disrupting traditional sell-in business models.**
    - ➢ *We announced Extreme Capital Solutions in April 2018. The offering includes subscription, capital leasing and usage business models that provide flexibility for partners and customers.*
  - **Growth of wireless devices continues to outpace hardwire switch growth.**
    - ➢ *We announced our 802.11ac Wave 2 wireless offering in late 2015 and plans to continue to advance our wireless portfolio of indoor and outdoor access points.*

The Extreme Strategy

We are focused on delivering end-to-end IP networking solutions for today's enterprise environments. From wireless and wired access technologies, through the campus, core and into the datacenter, Extreme is developing solutions to deliver outstanding business outcomes for our customers. Leveraging a unified management approach, both on premise and in the cloud, we continue to accelerate adoption and delivery of new technologies in support of emerging trends in enterprise networking. We continue to execute on our growth objectives by maximizing customer, partner, and shareholder value.

In fiscal 2014, we completed the acquisition of Enterasys Networks. In fiscal 2017, we completed the acquisition of the WLAN Business from Zebra. In fiscal 2018, we completed the acquisitions of the Campus Fabric Business from Avaya and the Data Center Business from Brocade. These acquisitions support our growth strategy to lead the enterprise network equipment market with end-to-end software-driven solutions for enterprise customers from the data center to the wireless edge. After the closing of the acquisitions of the Campus Fabric Business and Data Center Business, Extreme immediately became a networking industry leader with more than 30,000 customers. As a network switching leader in enterprise, datacenter and cloud, after closing of the Campus Fabric Business, we combine and extend our world-class products and technologies to provide customers with some of the most advanced, high performance and open solutions in the market as well as a superb overall customer experience. The combination of Extreme, the Campus Fabric Business and the Data Center Business is significant in that it brings together distinct strengths addressing the key areas of the network, from unified wired and wireless edge, to the enterprise core, to the data center and cloud to offer a complete, unified portfolio of software-driven network access solutions.

Provider of high quality, software-driven, secure networking solutions and the industry's #1 customer support organization

- Only multi-vendor network management with "single pane of glass".
- Delivering new releases of next generation portfolio organically and through acquisition.

Key elements of our strategy include:

- **Focus on being nimble and responsive to customers and partners, we call this "Customer-Driven Networking™."** We work with our customers to deliver software-driven solutions from the enterprise edge to the cloud that are agile, adaptive, and secure to enable digital transformation for our customers. We help our customers move beyond just "keeping the lights on", so they can think strategically and innovate. By allowing customers to access critical decision-making intelligence, we are able reduce their daily tactical work so they can spend their time on learning and understanding how to innovate their business with IT.
- **Enable a common fabric to simplify and automate the network.** With the acquisition of the Campus Fabric Business, Extreme now has access to field driven Campus and Data Center Fabric technologies. Fabric technologies virtualize the network infrastructure (decoupling network services from physical connectivity) which enables network services to be turned up faster, with lower likelihood of error. They make the underlying network much easier to design, implement, manage and troubleshoot.
- **Software-driven networking services-led solutions.** Our software-driven solutions provide visibility, control and strategic intelligence from the Edge to the Data Center, across networks and applications. Our solutions include wired switching, wireless switching, wireless access points and controllers. We offer a suite of products that are tightly integrated with access control, network and application analytics as well as network management. All can be managed, assessed and controlled from one single pane of glass.
- **Offer customers choice – cloud or on premise.** We leverage cloud where it makes sense for our customers and provide on premise solutions where customers need it. Our hybrid approach gives our customers options to adapt the technology to their business. At the same time, all of our solutions have visibility, control and strategic information built in, all tightly integrated with one single pane of glass. Our customers can understand what's going on across the network and applications in real time – who, when, and what is connected to the network, which is critical for BYOD and IoT.
- **Enable IoT without additional IT resources.** In a recent IoT IT infrastructure survey conducted in December 2016, enterprise IT decision makers across industry verticals indicated their preference to opt for their existing wireless connectivity infrastructure to support IoT devices. These preferences will place unprecedented demand on network administrators to enhance management capabilities, scalability and programmability of the enterprise networks they manage without additional IT resources.
- **Provide a strong value proposition for our customers.** Our cloud-managed wired and wireless networking solutions that provide additional choice and flexibility with on or off premise network, device and application management coupled with our award-winning services and support provide a strong value proposition to the following customers and applications:
    - Enterprises and private cloud data centers use our products to deploy automated next-generation virtualized and high-density infrastructure solutions.
    - Enterprises and organizations in education, healthcare, manufacturing, hospitality, transportation and logistics and government agencies use our solutions for their mobile campus and backbone networks.
    - Enterprises, universities, healthcare and hospitality organizations use our solutions to enable better visibility and control of their data processing and analytics requirements.
- **Provide high-quality customer service and support.** We seek to enhance customer satisfaction and build customer loyalty through high-quality service and support. This includes a wide range of standard support programs that provide the level of service our customers require, from standard business hours to global 24-hour-a-day, 365-days-a-year real-time response support.

- **Extend switching and routing technology leadership.** Our technological leadership is based on innovative switching, routing and wireless products, the depth and focus of our market experience and our operating systems - the software that runs on all of our Ethernet Switches. Our products reduce operating expenses for our customers and enable a more flexible and dynamic network environment that will help them meet the upcoming demands of IoT, mobile, and cloud, etc. Furthermore, our network operating systems, our primary merchant silicon vendor, and select manufacturing partners permit us to leverage our engineering investment. We have invested in engineering resources to create leading-edge technologies to increase the performance and functionality of our products, and as a direct result, the value of our solution to our current and future customers. We look for maximum synergies from our engineering investment in our targeted verticals.
- **Expand Wi-Fi technology leadership.** Wireless is today's network access method of choice and every business must deal with scale, density and BYOD challenges. The increase in demand being seen today, fueled by more users with multiple devices, increases the expectation that everything will just work. The network edge landscape is changing as the explosion of mobile devices increases the demand for mobile, transparent and always-on wired to wireless edge services. This new "unified access layer" requires distributed intelligent components to ensure that access control and resiliency of business services are available across the entire infrastructure and manageable from a single console. Our unified access layer portfolio provides intelligence for the wired/wireless edge
- **Continue to deliver unified management and a common fabric across the wired/wireless environment from the Data Center to the mobile Edge.** Our rich set of integrated management capabilities provides centralized visibility and highly efficient anytime, anywhere control of enterprise wired and wireless network resources.
- **Offer a superior quality of experience.** Our network-powered application analytics provide actionable business insight by capturing and analyzing context-based data about the network and applications to deliver meaningful intelligence about applications, users, locations and devices. With an easy to comprehend dashboard, our applications help businesses to turn their network into a strategic business asset that helps executives make faster and more effective decisions.

  Data can be mined to show how applications are being used enabling a better understanding of user behavior on the network, identifying the level of user engagement and assuring business application delivery to optimize the user experience. Application adoption can be tracked to determine the return on investment associated with new application deployment.

  Visibility into network and application performance enables our customers to pinpoint and resolve performance bottlenecks in the infrastructure whether they are caused by the network, application or server. This saves both time and money for the business and ensures critical applications are running at the best possible performance.
- **Software-driven networking solutions for the enterprise.** We are a software-driven networking solution company focused on the enterprise. We focus our R&D team and our sales teams to execute against a refined set of requirements for optimized return on investment, faster innovation, and clearer focus on mega trends and changes in the industry. As a software-driven networking company, we offer solutions for the entire enterprise network, the data center, the campus, the core and the WLAN.
- **Expand market penetration by targeting high-growth market segments.** Within the Campus, we focus on the mobile user, leveraging our automation capabilities and tracking WLAN growth. Our Data Center approach leverages our product portfolio to address the needs of public and private Cloud Data Center providers. Within the Campus we also target the high-growth physical security market, converging technologies such as Internet Protocol ("IP") video across a common Ethernet infrastructure in conjunction with technology partners.
- **Leverage and expand multiple distribution channels.** We distribute our products through select distributors, a large number of resellers and system-integrators worldwide, and several large strategic partners. We maintain a field sales force to support our channel partners and to sell directly to certain strategic accounts. As an independent Ethernet switch vendor, we seek to provide products that, when combined with the offerings of our channel partners, create compelling solutions for end-user customers.
- **Maintain and extend our strategic relationships.** We have established strategic relationships with a number of industry-leading vendors to both provide increased and enhanced routes to market, but also to collaboratively develop unique solutions.

We seek to differentiate ourselves in the market by delivering a value proposition based on a software-driven approach to network management, control and analytics.

Competition

The market for network switches, routers and software (including analytics) which is part of the broader market for networking equipment is extremely competitive and characterized by rapid technological progress, frequent new product introductions, changes in customer requirements and evolving industry standards. We believe the principal competitive factors in this market are:

- expertise and familiarity with network protocols, network switching/routing/wireless and network management;
- expertise and familiarity with application analytics software;
- expertise with network operations and management software;
- expertise in machine learning and artificial intelligence;
- product performance, features, functionality and reliability;
- price/performance characteristics;
- timeliness of new product introductions;
- adoption of emerging industry standards;
- customer service and support;
- size and scope of distribution network;
- brand name;
- breadth of product offering;
- access to customers; and
- size of installed customer base.

We believe we compete with our competitors with respect to many of the foregoing factors. However, the market for network switching solutions is dominated by a few large companies, particularly Cisco Systems, Inc., Dell, Hewlett-Packard Enterprise Co., Huawei Technologies Co. Ltd., Arista Networks Inc., Arris Corporation, and Juniper Networks Inc. Most of these competitors have longer operating histories, greater name recognition, larger customer bases, broader product lines and substantially greater financial, technical, sales, marketing and other resources.

We expect to face increased competition from both traditional networking solutions companies and Cloud platform companies offering Infrastructure-as-a-Service ("IaaS") and Platform-as-a-Service ("PaaS") products to enterprise customers. In that regard, we expect to face increased competition from certain Cloud Computing companies such as Amazon Web Services ("AWS"), Microsoft ("Microsoft Azure"), and Google Inc. ("Google Cloud Platform") providing a cloud-based platform of data center compute and networking services for enterprise customers.

With the acquisitions of assets from Zebra, Avaya and Brocade, we believe Extreme is uniquely positioned to address the most pressing market needs from the campus to the data center. Although we believe that our solutions and strategy will improve our ability to meeting the needs of our current and potential customers we cannot guarantee future success.

Restructuring

Fiscal year 2016

During fiscal 2016, we continued to realign our operations by abandoning excess facilities, primarily in San Jose, California; Salem, New Hampshire and Morrisville, North Carolina in addition to other smaller leased locations. These excess facilities represented approximately 32% of the floor space in the aggregate at these locations and included general office and warehouse space.

Fiscal year 2017

During fiscal 2017, we continued to realign our operations by continuing to review our excess facilities, expected sublease income, and implemented a reduction-in-force. We subleased our previous headquarters location at Rio Robles Drive in San Jose, California ("Rio Robles") and moved into a larger location at 6480 Via del Oro in San Jose, California ("Via del Oro") acquired as part of the WLAN Business acquisition. Additionally, due to the acquisitions of the Campus Fabric Business and the Data Center Business, there was a need to accommodate the increase in headcount. To address this need, the Company reoccupied a majority of the previously exited space in its Salem, New Hampshire location. In addition, we announced a reduction-in-force during the fiscal year affecting 90 employees.

Cost of Revenues and Gross Profit

The following table presents the gross profit on product and service revenue and the gross profit percentage of net revenues for the fiscal years 2018, 2017 and 2016 (dollars in thousands):

	Year Ended				Year Ended			
	June 30, 2018	June 30, 2017 (As adjusted)	$ Change	% Change	June 30, 2017 (As adjusted)	June 30, 2016 (As adjusted)	$ Change	% Change
Gross profit:								
Product	$ 407,393	$ 240,204	$167,189	69.6%	$ 240,204	$ 181,340	$ 58,864	32.5%
Percentage of product revenue	53.3%	52.2%			52.2%	46.9%		
Service	127,124	90,753	36,371	40.1%	90,753	84,063	6,690	8.0%
Percentage of service revenue	58.1%	61.9%			61.9%	63.2%		
Total gross profit	$ 534,517	$ 330,957	$203,560	61.5%	$ 330,957	$ 265,403	$ 65,554	24.7%
Percentage of net revenue	54.4%	54.5%			54.5%	51.1%		

Cost of product revenues includes costs of materials, amounts paid to third-party contract manufacturers, costs related to warranty obligations, charges for excess and obsolete inventory, scrap, distribution, product certification, amortization of developed technology intangibles, royalties under technology license agreements, and internal costs associated with manufacturing overhead, including management, manufacturing engineering, quality assurance, development of test plans, and document control. We outsource substantially all of our manufacturing. We conduct supply chain management, quality assurance, manufacturing engineering and document control at our facilities in San Jose, California, Salem, New Hampshire, China, and Taiwan.

Product gross profit increased to $407.4 million for the year ended June 30, 2018, from $240.2 million in the corresponding period of fiscal 2017, primarily due to higher revenues attributed to the acquisitions of the WLAN, the Campus Fabric and the Data Center Businesses and lower production costs due to cost reduction efforts. The increases in product gross profit were partially offset by increases in amortization of developed technology intangibles of $9.9 million, warranty charges of $7.2 million, royalty charges of $2.2 million and acquisition and integration related costs of $7.7 million including excess inventory charges related to the discontinuance of certain product lines due to the acquisitions of the Campus Fabric and the Data Center Businesses in excess of the same charges incurred related to the acquisition of the WLAN Business in the corresponding period in fiscal 2017.

Product gross profit increased to $240.2 million for the year ended June 30, 2017, from $181.3 million in the corresponding period of fiscal 2016. Product gross profit for the year ended June 30, 2017, was favorably impacted by an increase in product revenue of $73.5 million due primarily to the acquisition of the WLAN Business, lower amortization of developed technology intangibles of $8.3 million and more favorable manufacturing costs due to cost reduction efforts and lower warranty charges of $2.2 million. The increases in product gross profit were partially offset by integration costs of $5.0 million primarily related to excess inventory charges related to the discontinuance of certain product lines due to the WLAN Business acquisition and increased royalty charges of $2.6 million.

Our cost of service revenue consists primarily of labor, overhead, repair and freight costs and the cost of service parts used in providing support under customer maintenance contracts.

Service gross profit increased to $127.1 million for the year-ended June 30, 2018, from $90.8 million in the corresponding period of fiscal 2017, primarily due to the acquisitions of the WLAN, Campus Fabric and Data Center Businesses as a result of a higher number of maintenance contracts.

Service gross profit increased to $90.8 million for the year ended June 30, 2017, from $84.1 million in the corresponding period of fiscal 2016, primarily due to an increase in service revenue of $6.7 million related to the acquisition of the WLAN Business and the increased number of service contracts acquired.

Exhibit 28

Excerpts from Juniper Networks, Inc.'s Form 10-K Annual Report for the Fiscal Year Ended Dec. 31, 2018

UNITED STATES SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 10-K

(Mark One)

☒ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the fiscal year ended December 31, 2018

or

☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the transition period from_____ to_____

Commission file number 001-34501

JUNIPER NETWORKS, INC.

(Exact name of registrant as specified in its charter)

Delaware	**77-0422528**
(State or other jurisdiction of incorporation or organization)	*(I.R.S. Employer Identification No.)*
1133 Innovation Way	
Sunnyvale, California	**94089**
(Address of principal executive offices)	*(Zip code)*

(408) 745-2000
(Registrant's telephone number, including area code)

Securities registered pursuant to Section 12(b) of the Act:

Title of each class	**Name of each exchange on which registered**
Common Stock, par value $0.00001 per share	New York Stock Exchange

Securities registered pursuant to Section 12(g) of the Act: None

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ☒ No ☐
Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act. Yes ☐ No ☒

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filings requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T (§ 232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit such files). Yes ☒ No ☐

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K (§ 229.405 of this chapter) is not contained herein, and will not be contained, to the best of the registrant's knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K. ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, a smaller reporting company, or an emerging growth company. See the definitions of “large accelerated filer,” “accelerated filer,” “smaller reporting company”, and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large accelerated filer ☒	Accelerated filer ☐	Non-accelerated filer ☐	Smaller reporting company ☐	Emerging growth company ☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Act). Yes ☐ No ☒

The aggregate market value of voting common stock held by non-affiliates of the registrant was approximately $9,483,000,000 as of June 29, 2018, the last business day of the registrant’s most recently completed second fiscal quarter (based on the closing sales price for the common stock on the New York Stock Exchange on such date).

As of February 15, 2019, there were 347,922,460 shares of the registrant's common stock outstanding.

DOCUMENTS INCORPORATED BY REFERENCE

As noted herein, the information called for by Part III is incorporated by reference to specified portions of the registrant's definitive proxy statement to be filed in conjunction with the registrant's 2019 Annual Meeting of Stockholders, which is expected to be filed not later than 120 days after the registrant's fiscal year ended December 31, 2018.

Channel Sales Structure

A critical part of our sales and marketing efforts are our channel partners through which we conduct the majority of our sales. We utilize various channel partners, including, but not limited to the following:

- A global network of strategic distributor relationships, as well as region-specific or country-specific distributors who in turn sell to local VARs who sell to end-user customers. Our distribution channel partners resell routing, switching, and security products and services, which are purchased by all of our key customer verticals. These distributors tend to focus on particular regions or countries within regions. For example, we have substantial distribution relationships with Ingram Micro in the Americas and Hitachi in Japan. Our agreements with these distributors are generally non-exclusive, limited by region, and provide product and service discounts and other ordinary terms of sale. These agreements do not require our distributors to purchase specified quantities of our products or services. Further, most of our distributors sell our competitors' products and services, and some sell their own competing products and services.

- VARs and Direct value-added resellers, including our strategic worldwide alliance partners referenced below, resell our products to end-users around the world. These channel partners either buy our products and services through distributors, or directly from us, and have expertise in designing, selling, implementing, and supporting complex networking solutions in their respective markets. Our agreements with these channel partners are generally non-exclusive, limited by region, and provide product and service discounts and other ordinary terms of sale. These agreements do not require these channel partners to purchase specified quantities of our products or services. Increasingly, our Cloud and Service Provider customers also resell our products or services to their customers or purchase our products or services for the purpose of providing managed or cloud-based services to their customers.

- Strategic worldwide reseller relationships with established Juniper alliances, comprised of Dimension Data Holdings, or Dimension Data; Ericsson Telecom A.B., or Ericsson; International Business Machines, or IBM; and NEC Corporation. These companies each offer services and products that complement our own product and service offerings and act as a reseller, and in some instances as an integration partner for our products. Our arrangements with these partners allow them to resell our products and services on a non-exclusive and generally global basis, provide for product and service discounts, and specify other general terms of sale. These agreements do not require these partners to purchase specified quantities of our products or services.

Manufacturing and Operations

As of December 31, 2018, we employed 340 people in worldwide manufacturing and operations who manage our supply chain including relationships with our contract manufacturers, original design manufacturers, component suppliers, warehousing and logistics service providers.

Our manufacturing is primarily conducted through contract manufacturers and original design manufacturers in the United States, or U.S., China, Malaysia, Mexico, and Taiwan. As of December 31, 2018, we utilized Celestica Incorporated, Flextronics International Ltd., Accton Technology Corporation, and Alpha Networks Inc. for the majority of our manufacturing activity. Our contract manufacturers and original design manufacturers are responsible for all phases of manufacturing from prototypes to full production including activities such as material procurement, surface mount assembly, final assembly, test, control, shipment to our customers, and repairs. Together with our contract manufacturers and original design manufacturers, we design, specify, and monitor the tests that are required to ensure that our products meet internal and external quality standards. We believe that these arrangements provide us with the following benefits:

- We can quickly ramp up and deliver products to customers with turnkey manufacturing;

- We gain economies of scale by leveraging our buying power with our contract manufacturers and original design manufacturers when we manufacture large quantities of products;

- We operate with a minimum amount of dedicated space and employees for manufacturing operations; and

- We can reduce our costs by reducing what would normally be fixed overhead expenses.

Our contract manufacturers and original design manufacturers build our products based on our rolling product demand forecasts. Each contract manufacturer procures components necessary to assemble the products in our forecast and tests the products according to agreed-upon specifications. Products are then shipped to our distributors, VARs, or end-users. Generally, we do not own the components. Title to the finished goods is generally transferred from the contract manufacturers to us when the products leave the

We are dependent on contract manufacturers with whom we do not have long-term supply contracts, and changes to or disruptions in those relationships or manufacturing processes, expected or unexpected, may result in delays that could cause us to lose revenues and damage our customer relationships.

We depend on independent contract manufacturers (each of which is a third-party manufacturer for numerous companies) to manufacture our products. Although we have contracts with our contract manufacturers, these contracts do not require them to manufacture our products on a long-term basis in any specific quantity or at any specific price. In addition, it is time-consuming and costly to qualify and implement additional contract manufacturer relationships. Therefore, if we fail to effectively manage our contract manufacturer relationships, which could include failing to provide accurate forecasts of our requirements, or if one or more of them experiences delays, disruptions, or quality control problems in their manufacturing operations, or if we had to change or add additional contract manufacturers or contract manufacturing sites, our ability to ship products to our customers could be delayed. We have experienced in the past and may experience in the future an increase in the expected time required to manufacture our products or ship products. Such delays could result in supply shortfalls that damage our ability to meet customer demand for those products and could cause our customers to purchase alternative products from our competitors. Also, the addition of manufacturing locations or contract manufacturers or the introduction of new products by us would increase the complexity of our supply chain management. Moreover, a significant portion of our manufacturing is performed in China and other foreign countries and is therefore subject to risks associated with doing business outside of the United States, including import tariffs or regional conflicts. For example, the United States recently imposed a tariff on networking products imported from China; this includes certain products that we import into and sell within the United States. If we cannot mitigate the impact of the tariffs, the increased cost could translate into higher prices for our customers, reduced customer demand or increased cost of goods sold. In addition, increased costs of production or delays in production caused by any relocation of contract manufacturing facilities could impact the global competitiveness of our products. Each of these factors could adversely affect our business, financial condition and results of operations.

We are dependent on sole source and limited source suppliers, including for key components, which makes us susceptible to shortages, quality issues or price fluctuations in our supply chain, and we may face increased challenges in supply chain management in the future.

We rely on single or limited sources for many of our components. During periods of high demand for electronic products, component shortages are possible, and the predictability of the availability of such components may be limited. For example, we have recently experienced industry-wide supply constraints related to power management components. In addition, some components used in our networking solutions have in the past and may in the future experience extended lead times and higher pricing, given the demand in the market. Any future spike in growth in our business, the use of certain components we share in common with other companies, in IT spending or the economy in general, is likely to create greater short-term pressures on us and our suppliers to accurately forecast overall component demand and to establish optimal component inventories. If shortages or delays persist, we may not be able to secure enough components at reasonable prices or of acceptable quality to build and deliver products in a timely manner, and our revenues, gross margins and customer relationships could suffer. Additionally, if certain components that we receive from our suppliers have defects or other quality issues, we may have to replace or repair such components, and we could be subject to claims based on warranty, product liability, epidemic or delivery failures that could lead to significant expenses. We maintain product liability insurance, but there is no guarantee that such insurance will be available or adequate to protect against all such claims. We have experienced, and from time-to-time may experience, component shortages or quality issues that resulted, or could result, in delays of product shipments, revenue charges that impact our gross margins, and/or warranty or other claims or costs. We also currently purchase numerous key components, including ASICs and other semiconductor chips, from single or limited sources and many of our component suppliers are concentrated in China and Korea. In addition, there has been consolidation among certain suppliers of our components. For example, GLOBALFOUNDRIES acquired IBM’s semiconductor manufacturing business, Avago Technologies Limited acquired Broadcom Corporation and Intel Corporation acquired Altera Corporation. Consolidation among suppliers can result in the reduction of the number of independent suppliers of components available to us, which could negatively impact our ability to access certain component parts or the prices we have to pay for such parts. In addition, our suppliers may determine not to continue a business relationship with us for other reasons that may be beyond our control. Any disruptions to our supply chain could decrease our sales, earnings and liquidity or otherwise adversely affect our business and result in increased costs. Such a disruption could occur as a result of any number of events, including, but not limited to, increases in wages that drive up prices, the imposition of regulations, quotas or embargoes on components, labor stoppages, transportation failures affecting the supply chain and shipment of materials and finished goods, third-party interference in the integrity of the products sourced through the supply chain, the unavailability of raw materials, severe weather conditions, natural disasters, civil unrest, military conflicts, geopolitical developments, war or terrorism and disruptions in utility and other services.

The development of alternate sources for components is time-consuming, difficult, and costly. In addition, the lead times associated with certain components are lengthy and preclude rapid changes in quantities and delivery schedules. Also, long-term supply and maintenance obligations to customers increase the duration for which specific components are required, which may further increase

Exhibit 29

"OnePlus Breaks Into Top 5 Premium Phone Makers in US Market"

OnePlus Breaks Into Top 5 Premium Phone Makers in US Market

By Ryan Whitwam (https://www.extremetech.com/author/rwhitwam) on February 12, 2019 at 1:02 pm

21 Comments (https://www.extremetech.com/mobile/285635-oneplus-breaks-into-top-5-premium-phone-makers-in-us-market#disqus_thread)

OnePlus popped up about five years ago, talking a big game about shaking up the phone industry. Those early attempts to get attention were pretty cringeworthy, but the company has matured over the years and started producing extremely competitive phones. The prices are higher than they once were, but OnePlus is still clocking in less expensive than the phones from Samsung, LG, and Google. This approach is working, too. OnePlus (https://www.extremetech.com/tag/oneplus) points to new numbers from IDC that show it among the top five premium smartphone makers in the US (https://www.digitaltrends.com/mobile/oneplus-top-five-us/).

According to the Q4 2018 numbers, OnePlus is now the fifth largest smartphone maker in the US market for phones costing more than $500. That puts it up there with Samsung and Apple. However, OP's overall ranking is lower when you factor in cheap phones, which still sell in large numbers as flagship phones get ever more costly.

OnePlus' journey to this point has been meteoric, but it hasn't been free of drama. OnePlus started with the OnePlus One, a phone that offered nearly flagship-level specs for just $299. In those early days, OnePlus used an invite system to limit costs. That made the phones harder to buy, but it *tried* to get people excited by running contests that encouraged people to break their old phones and women to post selfies. Yeah, those were bad ideas.

Not all the bumps in the road were OP's doing, though. It launched with the Cyanogen OS build of Android, but Cyanogen canceled that partnership just months later. That sent OnePlus scrambling to develop its own version of Android. It came up with Oxygen OS. The first few builds were a bit rough, but it's evolved into one of the best OEM Android skins on the market. Today, all of OnePlus' phones are powered by Oxygen OS.

(https://www.extremetech.com/wp-content/uploads/2018/08/587182-oneplus-6.jpg)

All OnePlus phones from OnePlus 3 onward were available without invites, but still only unlocked. The price also started to creep upward. The company still claimed strong sales, particularly in India.

The OnePlus 6T launched late last year (https://www.extremetech.com/mobile/279976-the-oneplus-6t-launches-today-on-t-mobile-or-unlocked), and this is what catapulted the company into the upper echelons of premium smartphone makers. At $550, the 6T is still several hundred dollars less

expensive than other high-end smartphones, and the compromises to reach that price are relatively minor. It's also available on T-Mobile, OP's first US carrier partnership. The unlocked version works on Verizon as well.

In the coming months, OnePlus is expected to release the OnePlus 7 with a notchless slider design. A separate 5G smartphone for select US carriers may also be in the cards.

Now read:

- OnePlus 5 and 5T Will Get Faster Android Updates With Project Treble Support (https://www.extremetech.com/mobile/272885-oneplus-5-and-5t-will-get-faster-android-updates-with-project-treble-support)
- OnePlus Will Be Among the First to Launch a 5G Phone (https://www.extremetech.com/mobile/279422-oneplus-will-be-among-the-first-to-launch-a-5g-phone)
- Android or iOS: Who's Winning the Mobile Speed Race? (https://www.extremetech.com/mobile/263966-android-ios-whos-winning-global-speed-race)

Exhibit 30

"Who is BBK, The World's Third Largest Phone Manufacturer?"

FEATURES NEWS October 20, 2017

Who is BBK, the world’s third largest phone manufacturer?

Robert Triggs

The smartphone market seems to be a perpetual fight for third place behind Samsung and Apple. Huawei has been trying to set itself up as the third largest brand, with successful pushes into the Asian, European, and now even U.S. markets. But they've got some relatively lesser-known competition to confront before they can claim the title of third— BBK Electronics.

BBK is a Chinese multinational corporation that owns a number of popular brands across various consumer electronics markets, including headphones, Blu-ray players, and smartphones. It owns two major smartphone brands and one fan favourite— Oppo, Vivo, and OnePlus.

Who is BBK?

BBK Electronics has been operating in various sections of China's electronics industry since around the 1990's. The company is spearheaded by reclusive billionaire Duan Yongping. After successfully generating more than 1 billion Yuan from the "Subor" gaming console, a competitor to the Nintendo Entertainment System, Duan left his position running a Chinese factory in 1995. He then started the company Bubugao, which would eventually become BBK. The company now owns factories spread over 10 hectares of land and more than 17,000 employees.

BBK Electronics began by manufacturing a range of CD, MP3, and DVD players, along with other household appliances, which appeared under a range of global brands. In 2004 Duan founded Oppo with CEO Tony Chen. Oppo built on Duan's experience in the video market by selling DVD and Blu-ray players, before moving into the smartphone market.

Vivo appeared a little later in 2009, and was founded by Duan and Vivo CEO Shen Wei. The first Vivo smartphones appeared in 2011 with a focus on ultra-slim form factors, while relying on celebrity endorsements to capitalize on the smartphone boom.

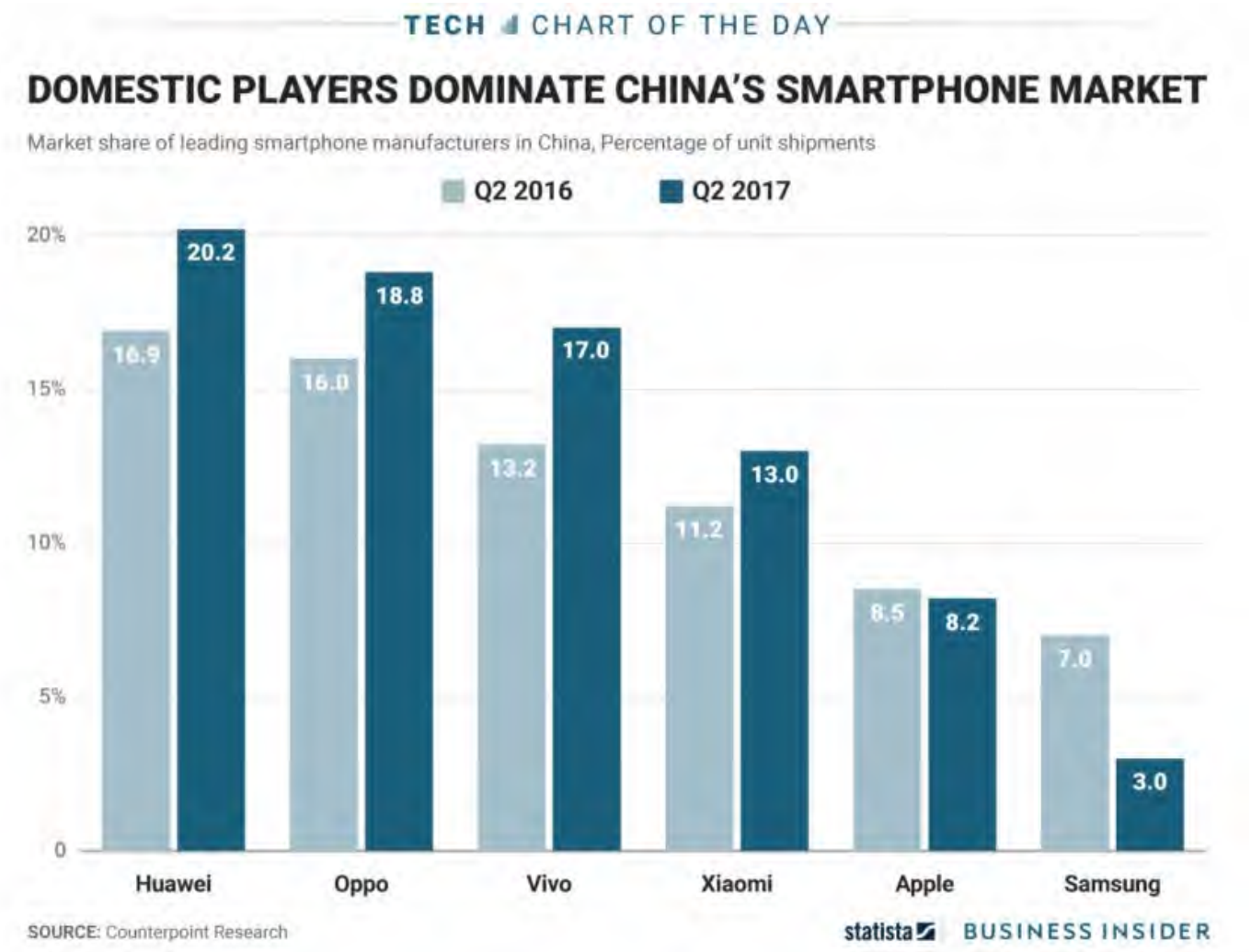
OnePlus, the BBK brand that Western customers might be most familiar with, wasn't started by Duan. It was founded by former Oppo vice president Pete Lau and co-founder Carl Pei in 2013, and is a subsidiary of Oppo. That still means it's owned by parent company BBK. OnePlus is arguably the most premium brand of

the three, however it takes a different approach to Oppo and Vivo's retail based business model. OnePlus primarily targets online sales via platforms like Amazon, which has helped BBK enter European and US markets.

Second or third place, depending on who you ask

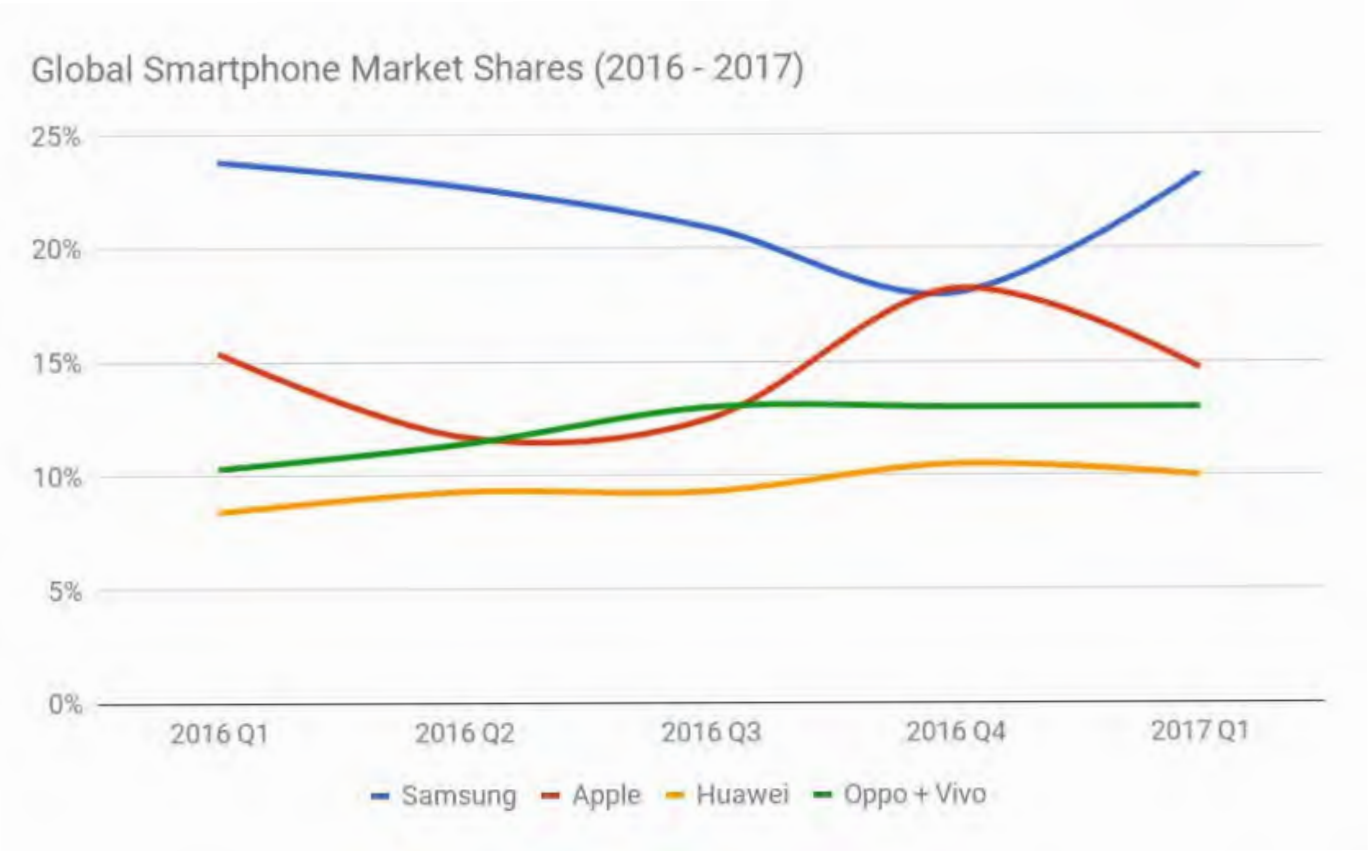
When it comes to smartphones, BBK Electronics is a big deal, even though most consumers have never heard of it. Oppo and Vivo have long been major players not just in the Chinese smartphone market, but internationally too.

In China, Oppo and Vivo have managed to surpass the growth rate of the once seemingly invincible Xiaomi by building a network of local stores, while its competitor focused on its efforts online. Apple and Samsung have struggled to keep pace with the cost competitive nature of China's homegrown mobile brands, including those in the BBK network. According to Counterpoint Research, Huawei is the biggest single brand with some 20.2% of China's market, but Oppo and Vivo are both very close behind on 18.8% and 17.0% respectively. Combined, BBK's smartphone brands have a comfortable lead with 35.8% of China's huge smartphone market.



Turning to the global outlook. In Q1 2017, Gartner research revealed that Oppo shipped around 30.9 million smartphones, with Vivo not far behind on 25.8 million. That's a combined total of 56.7 million. By comparison, Samsung shipped 78.6 million phones in the same quarter and Apple 51.9 million. BBK companies actually shipped more than Apple in Q1 2017, arguably putting them in second place, according to Gartner.

A similar report by IDC also paints a close picture, but with Apple retaining a small lead. According to its data, in Q1 2017 Samsung accounted for 23.3% of the global market, Apple on 14.7%, Huawei 10.0%, Oppo 7.5%, and Vivo 5.5%. Combined that would give BBK a market share of 13 percent, putting the company just behind Apple, but ahead of Huawei. OnePlus' market share isn't expected to account for even 1% of global sales, so it makes no meaningful difference to the rankings.



Market estimates always have some margin of error, but the data seems to suggest a close race for second between BBK and Apple. Throw Huawei into the mix and we're looking at three major companies all vying to close that gap on Samsung. That's a different picture than when looking at these brands individually, which sets the situation up as a simple first, second, and third ranking.

Looking forward

BBK Electronics isn't seemingly satisfied with just having a strong lead in China. The company recently overtook Samsung as the largest manufacturer in India, a key growth market. It also has a new phone brand named ikoo. This fourth smartphone sub-brand is looking to leverage experience in children's educational electronic toys to create the world's first education handset.

By spreading itself across multiple brands, BBK has managed to tailor its products to suit various market segments. The strategy has clearly paid off in China. Whether or not it will work in Western markets remains to be seen.

FEATURES NEWS

Tagged: OnePlus, Oppo, Vivo

Exhibit 31

"Meet the 'Godfather' of China's Smartphone Industry"

SCMP.COM

South China Morning Post

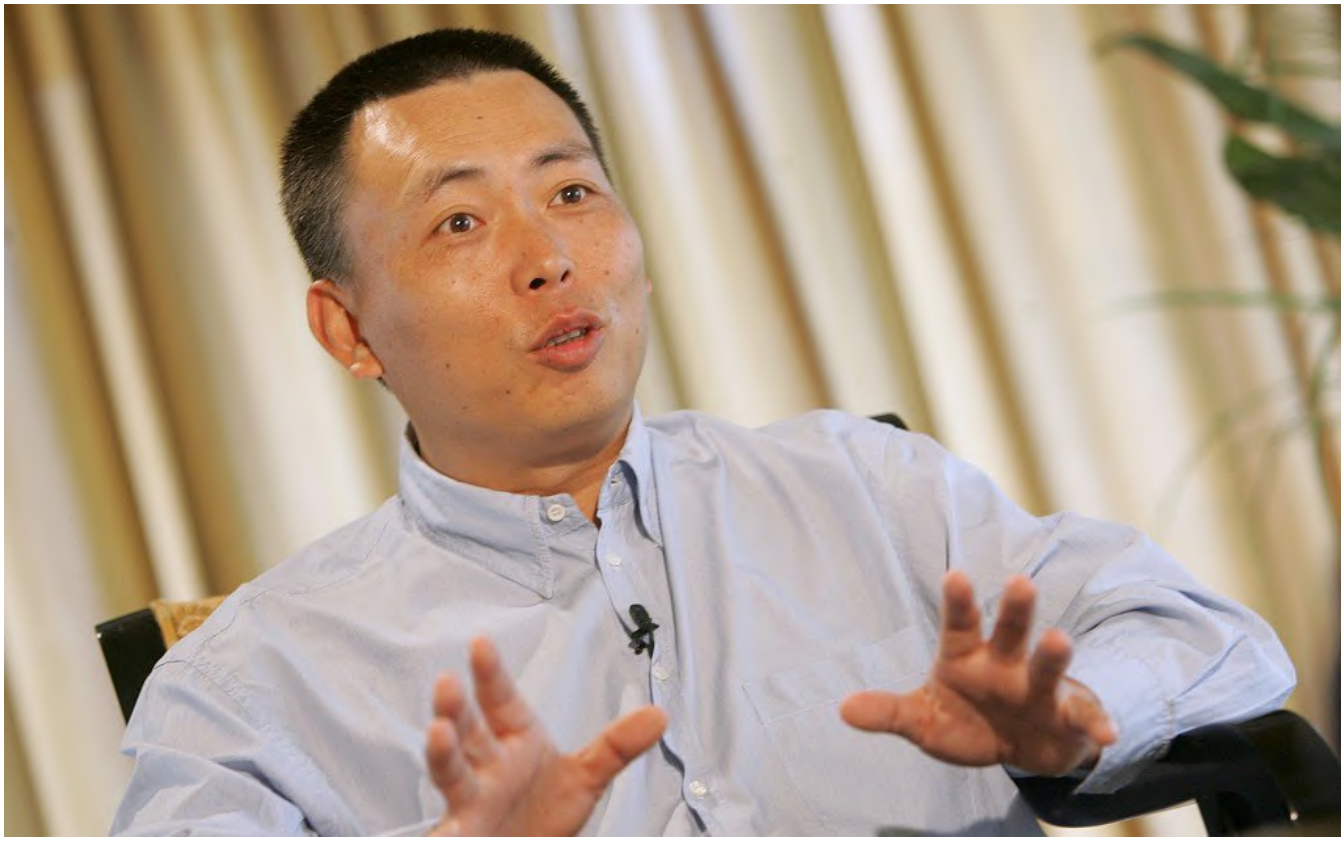
Big Tech

Meet the ‘godfather’ of China’s smartphone industry

Duan Yongping is the founder and chairman of Dongguan-based BBK Electronics Corp
Privately held BBK is behind smartphone brands Oppo, Vivo, OnePlus and Realme

Topic | Smartphones

Li Tao
Published: 6:02am, 4 Feb, 2019



Over a span of about 10 years, Chinese smartphone brands have not only topped sales in their home market, but also outshone major foreign rivals in many emerging and developed economies.

The success of four of those brands – Oppo and Vivo as well as recently established OnePlus and Realme – can be directly attributed to the guiding hand and investment savvy of reclusive Chinese billionaire entrepreneur, investor and philanthropist Duan Yongping.

He is the founder and chairman of privately held BBK Electronics Corp, a 24-year-old company based in the southern coastal city of Dongguan that now runs one of the world’s largest and most sophisticated electronics supply chains behind the production of a range of smartphones for the global market.

Duan, who will turn 58 years old next month, is widely regarded as the "godfather" of the Chinese smartphone industry for developing two brands, Oppo and Vivo, as large global players competing against the likes of Samsung Electronics, Apple, LG Electronics and mainland rival Huawei Technologies. OnePlus and Realme, which are backed by BBK and other investors, look to be the next big Chinese brands to conquer international markets.

Attempts to reach Duan and BBK were unsuccessful. The Chinese billionaire, who was interviewed by Bloomberg in 2017, was identified last year as an early investor in Pinduoduo, China's third largest e-commerce company, which was founded by his friend and protégé Colin Huang Zheng. Duan's net worth was estimated at 10 billion yuan (US$1.5 billion), according to the 2018 *Hurun China Rich List*.

In September last year, Duan also had a well-publicised conversation with Chinese students at Stanford University in Palo Alto, California, where his family lives. Duan and wife Liu Xin, a former journalist, had set up their family's Enlight Foundation to provide Chinese students undergraduate scholarships and graduate fellowships at the university's School of Engineering.

Duan first made international headlines near the end of June 2006, when he agreed to pay a then-record amount of US$620,100 in a bidding on eBay to have a power lunch at a New York steakhouse with renowned billionaire investment guru Warren Buffett, the chairman and chief executive of Berkshire Hathaway.

Behind the rise of China's smartphone brands lies growing unease over country's tech gains
[1]

"I've learned so much from Warren Buffett and his investment philosophy. I want a chance to say thank you," Duan said in a *South China Morning Post [2]* report [3] in July of that year. Apart from his wife, Duan brought six friends to that lunch, including Huang.

Born in March 1961 into a modest family in Nanchang, capital of Jiangxi province in southeast China, Duan in 1978 entered Zhejiang University in the eastern city of Hangzhou, where he majored in wireless electronics engineering.

After a short stint as a teacher at the adult education centre of the Beijing Radio Tube Factory, Duan pursued further studies at Beijing’s elite Renmin University of China, formerly known as People’s University, where he earned a master’s degree in economics in 1989.

Oppo was the world’s fifth largest smartphone supplier in 2018, according to data from Counterpoint Research. Photo: Reuters

That same year, he joined Zhongshan Yihua Group, located in the southern coastal province of Guangdong, to manage an ailing factory and turned it into a profitable business. He set up a unit that made cheap video game consoles, Subor Electronics Industry Corp, where he served as its chief executive.

Subor had much success in making education consoles, or learning machines, which were cheap copycats of Nintendo’s Famicom computers. That popular device, which was known as “Little Tyrant” in China and endorsed by Hong Kong martial arts superstar Jackie Chan at the time, helped Yihua achieve an annual profit of about 1 billion yuan (US$148 million) in 1995, compared with a loss of 2 million yuan when Duan joined the firm in 1989, according to a report by *Week in China* last year.

Despite that success, Duan had a public falling out with Yihua after his plan to spin off Subor and get a stake in the new company was rejected, the report said. He left Yihua in August 1995 and later that year, established electronics firm BBK, in which he had a controlling 70 per cent stake.

Vivo was the third biggest smartphone brand in China last year, according to research firm Canalys. Photo: Handout

Duan divided BBK’s business into three segments: education electronics, led by Huang Yihe; audiovisual, which made VCD and DVD players, under Chen Mingyong; and communications, which made mobile phones and cordless telephones, under Shen Wei. BBK had early success with its VCD and DVD players, becoming the leading vendor of those devices in China.

In 1999, Duan introduced a partnership programme that eventually led to the creation of independent business entities and reduction of his BBK stake to about 17 per cent. That led to Oppo Electronics Corp being founded in 2004 by Chen, while Vivo Communication Technology was formed by Shen in 2009. Pete Lau, the founder and chief executive of OnePlus, and Sky Li Bingzhong, founder of Realme, previously worked as vice-presidents at Oppo.

In his interview with Bloomberg, Duan said making mobile phones was not exactly his expertise, but reckoned his company could do well in the industry. That decision proved prescient, as sales of Chinese-brand Android smartphones took off when 3G and later 4G mobile networks were rolled out across the country.

Chinese smartphone brand Oppo doubles R&D investment to keep up with rivals ahead of 5G deployment
[4]

Demand for Chinese-brand mobile phones doubled each year between 2010 and 2012 during the period when 3G mobile services were being rolled out across the country, but gradually slowed down from 2013 ahead of the deployment of faster 4G services by the mainland’s three mobile network operators.

With the world’s biggest internet population and smartphone market, China had as many as 300 domestic mobile phone companies about three years ago. Cutthroat competition reduced that number to about 200 last year, as Chinese consumers bought fewer smartphones and the economy grew at a slower pace.

Only bet on the things you understand
Duan Yongping, chairman of BBK Electronics Corp

The larger, deep-pocketed Chinese smartphone suppliers have won a big chunk of the domestic market through aggressive promotions, advanced designs and features, and offering a wide array of models in a range of prices to entice both younger and affluent buyers.

Oppo and Vivo, respectively, were China’s second and third biggest smartphone suppliers in 2018, with a combined 40 per cent market share, according to estimates by research firm Canalys. They were behind market leader Huawei, but ahead of Xiaomi and Apple in a year when domestic smartphone shipments fell to 396 million units, compared with 459 million in 2017.

An employee tests the cameras of OnePlus smartphones at the company’s manufacturing facility in the southern coastal city of Dongguan, in Guangdong province. Photo: Bloomberg

In the global smartphone market last year, Oppo and Vivo took the fifth and six spots, respectively, with a combined 15 per cent share, according to data from Counterpoint Research. It said the top four-ranked vendors last year were Samsung, Apple, Huawei and Xiaomi.

Duan described the success of BBK along with sister brands Oppo and Vivo as no accident even if they were latecomers to the smartphone industry, according to a transcript of his talk with Stanford students last year. He attributed this to a focus on closely screening partners and suppliers, building “a great reputation”, making changes when something goes wrong and *benfen*, which loosely translates to integrity or honesty.

Vivo aims for high-end segment with premium, hi-tech handset sporting large dual displays

[5]

"In our early years, we often said our products provide good value at a cheap price," Duan said. "But over the years, I've learned that we were just making excuses for inferior products."

More than marketing and promotions, Duan said the goal was to focus on making a good products that meets users' requirements, whether in the low-end or high-end segment of the smartphone market.

China's OnePlus to launch first 5G smartphone in Europe with British carrier EE in 2019

[6]

Lau referred to *benfen* numerous times in an interview with the *Post* last year as the moral code that guides OnePlus, which he said helped the company gain the trust of consumers in the US and other overseas markets.

Duan, who emigrated to the US in 2002 to join his family, said he frowns on making speculative investments. "Only bet on the things you understand," he said. "Focus on understanding the business model and how the business makes money. Ninety-five per cent of investors focus on what the market will do. That's wrong."

Source URL: https://scmp.com/tech/big-tech/article/2184877/meet-godfather-chinas-smartphone-industry

Links
[1] https://www.scmp.com/tech/gear/article/2184131/behind-rise-chinas-smartphone-brands-lies-growing-unease-over-countrys
[2] https://www.scmp.com/article/556023/no-shortage-tips-buffett-lunch
[3] https://www.scmp.com/article/556023/no-shortage-tips-buffett-lunch
[4] https://www.scmp.com/tech/apps-social/article/2179613/chinese-smartphone-brand-oppo-doubles-rd-investment-keep-rivals
[5] https://www.scmp.com/tech/article/2177588/vivo-aims-high-end-segment-premium-hi-tech-handset-sporting-large-dual-displays
[6] https://www.scmp.com/tech/gear/article/2176545/chinas-oneplus-launch-first-5g-smartphone-europe-british-carrier-ee-2019

Exhibit 32

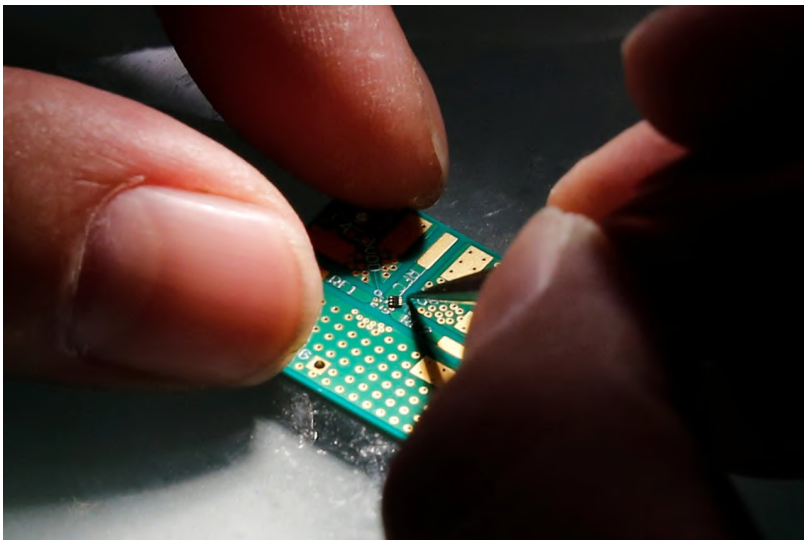
"China's Tsinghua Unigroup to Build $30 Billion Memory-Chip Factory in Nanjing"

https://www.wsj.com/articles/chinas-tsinghua-unigroup-to-build-30-billion-memory-chip-factory-in-nanjing-1484828235

TECH

China's Tsinghua Unigroup to Build $30 Billion Memory-Chip Factory in Nanjing

China is looking to diminish its dependence on U.S. chip manufacturers



A researcher plants a semiconductor on an interface board at a Tsinghua Unigroup research centre in Beijing. The company announced a $24 billion memory chip factory in Wuhan last March. PHOTO: KIM KYUNG-HOON/REUTERS

Updated Jan. 19, 2017 10:48 p.m. ET

BEIJING—China's flagship state-owned chip maker Tsinghua Unigroup said it plans to build a $30 billion memory-chip factory in Nanjing, its latest investment as China moves to diminish its dependence on U.S. chip manufacturers.

After several of its international chip deals were blocked by foreign governments, Tsinghua Unigroup has focused more on acquiring overseas talent and building its own plants.

This new planned plant comes after Tsinghua Unigroup announced a $24 billion memory chip factory in a different Chinese city, Wuhan, last March.

The U.S. is particularly wary about China's chip investments because semiconductors are one of the few sectors that the U.S. still manufactures competitively at home. Chips are the brains inside all computing devices and are an expensive technology that few companies can make.

Chinese officials say they need to be able to make the technology themselves to ensure national security. Beijing launched a $160 billion plan in 2014 to increase its share of domestically made

chips in its market from around 10% now to 70% over the next decade.

RELATED ARTICLES

- China's Tsinghua Unigroup Buys Small Stake in U.S. Chip Maker Lattice
- China's Tsinghua Unigroup to Build Memory Chip Factory
- China's Tsinghua Unigroup Plans to Buy Stakes in Taiwan Chip-Packaging Companies

An Obama administration advisory panel recommended this month that the U.S. tighten restrictions on Chinese chip investment in the U.S., citing national security reasons.

Tsinghua Unigroup said in a statement on its website that it will invest $30 billion in a factory in Nanjing to make storage chips, with monthly production capacity of 100,000 wafers. The technology, 3D-NAND and DRAM, is used in smartphones and other devices to store data.

In October 2015, Tsinghua Unigroup hired Charles Kau, former chairman of Taiwan's Inotera Memories Inc., as a vice chairman. Inotera is a joint-venture of Micron Technology Inc., a U.S. company that Tsinghua Unigroup unsuccessfully tried to acquire.

Other hires of Taiwan industry veterans followed. Tsinghua Unigroup said that it has executives including Shih-wei Sun, former chief executive of chip manufacturer United Microelectronics Corp. , James Shih, a former vice president of memory chip maker Nanya Technology Corp. , and Yuan Dih-wen, former senior executive of Taiwanese mobile chip designer MediaTek Inc.

—Eva Dou and Yang Jie

Exhibit 33

Tsinghua Holdings Co. Ltd.'s
"Products and Technological Services" Webpage

Products and Technological Services

Globalization is one of the important development strategies of Tsinghua Holdings Co Ltd. Through multiple measures such as product exportation, technological services and international M&A, Tsinghua Holdings has built an international network and industrial layout across more than 150 countries and regions. It strives to improve its international reputation with top technologies, outstanding products and good services.

● Tsinghua Unigroup has acquired listed companies including Spreadtrum Communications Inc, RDA Microelectronics and Tongfang Guoxin Electronics Co Ltd. It also holds stock in New H3C, cooperates with Intel and participates in Powertech Technology Inc, Siliconware Precision Industries Co Ltd and ChipMOS Technology Inc. Its products are sold in nearly 100 countries and regions throughout the world and its clients include over 80 percent of the Global Fortune 500 companies. Moreover, it has established chip and Internet product R&D centers in a dozen countries, including the US and Finland.

● The security inspection products and services of Nuctech Company Limited are accessible in 150 countries and regions. The company has the world's largest market share of large container inspection systems. It provides security services for international and domestic events.

● The China National Knowledge Infrastructure, operated by Tongfang Knowledge Network, has built "CNKI digital library" with the largest amount of full-text information in the world, with users from different walks of life in China and over 40 other countries and regions. It draws on 76 percent of the globe's top 500 universities.

● Tus-Holdings Co Ltd cooperates with foreign countries such as Russia, Spain and South Korea to export TusPark's advanced concepts and development models. It has established two Sino-US cross-border incubation bases in Silicon Valley, which serve as bridges, linking good science and technology with innovative people. The company strives to be a super incubation platform for global innovation and entrepreneurship.

BUSINESS

Incubators

Hi-Tech Industries

Innovation Services

SPECIALS

● Tongfang Technovator's comprehensive, integrated service network for city energy conservation covers more than 60 countries and regions in the Middle East, North America and Europe.

● Global Safety Technology Co Ltd is China's first supplier of public safety emergency response solutions. Its products and services are exported to foreign countries such as Ecuador, Venezuela, Trinidad, and Tobago to build public security emergency command and control systems.

● The biochip related products and technologies of CapitialBio Corporation are accessible in over 30 countries and regions.

● Chengzhi Shareholding Co Ltd is a main supplier of L-glutamine and D-ribose in the global market, and its market share of D-ribose crystal exceeds 50 percent globally.

● Xuetangx.com, a subsidiary of MOOC-CN Education, has brought global high quality educational resources together, with a large number of users from more than 200 countries and regions.

● Tsinghua University Press has hundreds of print copyrights internationally, including in the US, UK, Japan, Singapore, South Korea and Thailand. Its English-version works and journals on science and technology sell well around the world.

● Huahuan Electronics Co Ltd focuses on information networks to develop various pieces of equipment for communication, transportation and access.

0

Tsinghua Holdings boosts technology and innovation along the Belt and Road

View All

Exhibit 34

"Shenzhen Government Takes Control of China's Leading Chip Maker Tsinghua Unigroup"

SCMP.COM

South China Morning Post

China Business

Shenzhen government takes control of China's leading chip maker Tsinghua Unigroup

Tsinghua Unigroup is the third-largest smartphone chip maker in the world

Move part of a campaign to reduce corruption at university-owned enterprises

Topic | State-owned enterprises

Yujing Liu

Published: 9:15pm, 26 Oct, 2018

China's Tsinghua University will reduce its stake in the mainland's leading chip maker Tsinghua Unigroup amid a central government campaign to downsize the billions of dollars of corporate assets owned by public universities.

Tsinghua Holdings, which is owned by the public university, has agreed to transfer a 36 per cent stake in Unigroup to Shenzhen Investment Holdings, owned by the southern city's government agency overseeing state-owned assets, according to statements published by Unigroup's three Shenzhen-listed subsidiaries on Friday.

Tsinghua Holdings will retain a 15 per cent stake, according to the statements.

The campaign started to gain momentum since last June, when the Communist arty's anti-corruption watchdog found "high corruption risks" and ismanagement problems" at school-affiliated enterprises run by 13 out of the 14 universities it inspected. Tsinghua was the only school not named and shamed.

The party's reform policy formulation body released a guideline in May this year to call for tightened supervision and deeper reform of such enterprises, which are mostly in the hi-tech industry, as well as a clearer division between the schools' education and business operations.

Transferring company stakes to government-owned investment platforms is seen as one of the solutions that will also enhance the companies' competitiveness.

Tsinghua Unigroup shipped a total of 3.4 billion smartphone chips last year, making it the third largest mobile chip producer in the world, chief executive Zhao Weiguo said during a conference in August.

Tsinghua Holdings had previously signed agreements to transfer the stake to government-backed companies in the southern province of Hainan and Suzhou, Jiangsu province in eastern China in September. But they have since been terminated, according to the statements which did not provide the reasons behind its switch to Shenzhen.

Unisplendour Technology, a subsidiary suspended trading of its shares on Friday following the announcement.

https://www.scmp.com/tech/science-research/article/2161056/tsinghua-unigroup-president-calls-coexistence-foreign-chip
[1]

Source URL: https://scmp.com/business/china-business/article/2170440/shenzhen-government-takes-control-chinas-leading-chip-maker

Links
[1] https://www.scmp.com/tech/science-research/article/2161056/tsinghua-unigroup-president-calls-coexistence-foreign-chip

This article appeared in the South China Morning Post print edition as: Shenzhen to get 36pc stake in Tsinghua Unigroup

Exhibit 35

"Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology"
by Interos Solutions, Inc.

Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology

APRIL 2018

Principal Author

Tara Beeny, Senior Business Analyst, Interos Solutions, Inc.

Subject Matter Experts

Jennifer Bisceglie, CEO, Interos Solutions, Inc.

Brent Wildasin, Managing Director, Interos Solutions, Inc.

Dean Cheng, Independent Contractor

Interos Solutions, Inc.

1725 Duke Street, Suite 510

Alexandria, VA 22314

PREPARED FOR THE U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

Table of Contents

List of Tables

List of Exhibits

Acronyms

3GPP	Third Generation Partnership Project
5G	fifth generation
CAS	Chinese Academy of Sciences
CETC	China Electronics Technology Group Corporation
CNCI	Comprehensive National Cybersecurity Initiative
CNITSEC	China Information Technology Evaluation Center
CNSS	Committee on National Security Systems
COTS	commercial off-the-shelf
CSF	Cybersecurity Framework (NIST)
DFARS	Defense Federal Acquisition Regulation Supplement
DHS	Department of Homeland Security
DoD	Department of Defense
DRC	Democratic Republic of the Congo
FDI	foreign direct investment
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FITARA	Federal Information Technology Acquisition Reform Act
GAO	Government Accountability Office
GSA	General Services Administration
HP	Hewlett-Packard
ICT	information and communications technology
IDC	International Data Corporation
IoT	Internet of Things
IP	intellectual property
IT	information technology
ITU	International Telecommunication Union
LCD	liquid crystal display
NIST	National Institute of Standards and Technology

NIST SP	NIST Special Publication
NSA	National Security Agency
NSS	national security systems
OECD	Organisation for Economic Co-operation and Development
OEM	original equipment manufacturer
OMB	Office of Management and Budget
PLA	People's Liberation Army
PRC	People's Republic of China
R&D	research and development
SCRM	supply chain risk management
SD	Specialized Disclosure (SEC form)
SEC	Securities and Exchange Commission
SOE	state-owned enterprise
TRM	Technical Reference Module
VA	Department of Veterans Affairs
ZTE	Zhongxing Telecommunications Corporation

Executive Summary

The U.S. government needs a national strategy for supply chain risk management (SCRM) of commercial supply chain vulnerabilities in U.S. federal information and communications technology (ICT), including procurement linked to the People's Republic of China (China or PRC). This strategy must include supporting policies so that U.S. security posture is forward-leaning, rather than reactive and based on responding to vulnerabilities, breaches, and other incidents after they have already damaged U.S. national security, economic competitiveness, or the privacy of U.S. citizens.

This study uses a comprehensive definition of "U.S. government ICT supply chains" that includes (1) primary suppliers, (2) tiers of suppliers that support prime suppliers by providing products and services, and (3) any entities linked to those tiered suppliers through commercial, financial, or other relevant relationships. U.S. federal government ICT supply chains are multi-tiered, webbed relationships rather than singular or linear ones. The supply chain threat to U.S. national security stems from products produced, manufactured, or assembled by entities that are owned, directed, or subsidized by national governments or entities known to pose a potential supply chain or intelligence threat to the United States, including China. These products could be modified to (1) perform below expectations or fail, (2) facilitate state or corporate espionage, or (3) otherwise compromise the confidentiality, integrity, or availability of a federal information technology system.

Software supply chain attacks will become easier—and more prevalent—as developing technologies such as fifth generation (5G) mobile network technology and the Internet of Things (IoT) exponentially increase avenues for attack.[1] Gartner, an American information technology (IT) research and advisory firm, predicts that by 2021 there will be 25.1 billion IoT units installed,[2] and by 2020, IoT technology will be in 90 percent of new computer-enabled product designs.[3] This growth in IoT connectivity will have an important impact on the ICT SCRM challenge. Relevant to this report, increasing IoT installation will expand the attack surface of federal ICT networks while decreasing the time required to breach them, yet the time required to detect those breaches is not decreasing. The responsibility of both the public and private sectors in increasing their approach to risk awareness and management in the commercial technology supply chain cannot be overstated.

China did not emerge as a key node on the global ICT supply chain by chance. The Chinese government considers the ICT sector a "strategic sector" in which it has invested significant state capital and influence on behalf of state-owned ICT enterprises. China has long-standing policies encouraging ICT manufacturing and development. These policies offer incentives for foreign companies to produce ICT in China, while at the same time pursuing opportunities to obtain key intellectual property and technology from those companies with the ultimate goal of indigenizing these technologies. Since 2013, China has accelerated its efforts at indigenous production and independence. This shift has made for a more restrictive environment for companies doing business in China, extracting concessions from large multinationals in exchange for market access. At the same time, China has expanded its efforts to obtain economic advantage by pursuing knowledge of key technologies through corporate acquisitions and by using the economic power of Chinese companies as tools of the state. The PRC government justifies these policies in terms of ensuring China's own national security, but China's policies related to prioritizing indigenous production, extracting concessions from multinationals, using Chinese companies as state tools, and targeting U.S. federal networks and the networks of federal contractors have heightened risks to the U.S. ICT supply chain, and to U.S. national and economic security. New policies requiring companies to surrender source code, store data on servers based in China, invest in Chinese companies, and allow the Chinese government to conduct security audits on their products open federal ICT providers—and the federal ICT networks they supply—to Chinese

1 The Internet of Things refers to a system of interrelated computing devices, mechanical and digital machines, objects, and living beings equipped with network connectivity that enables them to connect and exchange data.

2 Peter Middleton et al., "Forecast: Internet of Things–Endpoints and Associated Services, Worldwide, 2017," Gartner, Inc., December 21, 2017, https://www.gartner.com/doc/3840665/forecast-internet-things--endpoints.

3 Benoit J. Lheureux et al., "Predicts 2018: Expanding Internet of Things Scale Will Drive Project Failures and ROI Focus," Gartner, Inc., November 28, 2017, https://www.gartner.com/doc/3833669/predicts--expanding-internet-things.

cyberespionage efforts and intellectual property theft. China also continues to target U.S. government contractors and other private sector entities as part of its efforts to gain economic advantage and pursue other state goals.

RECOMMENDATIONS FOR A NATIONAL SCRM STRATEGY

Effective SCRM is the ability to anticipate future developments in supply chains, identity potential threats to supply chains, develop threat profiles, and mitigate or address future threats to the supply chain. Federal government laws and policies do not address SCRM comprehensively. The evolution of global production and manufacturing of ICT products and the nature of federal ICT modernization efforts means new products entering the federal information systems and national security systems have increasingly complex and globalized supply chains, many of which originate with commercial suppliers sourcing from China. It is unlikely that political or economic shifts will cause global ICT manufacturers to dramatically reduce their operations in China or their partnerships with Chinese firms. How, then, should the U.S. government manage risks associated with Chinese-made products and services and the participation of Chinese companies in its ICT supply chains? Federal ICT supply chain risks can be best managed by embracing an adaptive SCRM process, centralizing the leadership of federal ICT SCRM efforts, linking federal regulations to appropriations, promoting supply chain transparency, and crafting forward-looking policies.

EMBRACE AN ADAPTIVE SUPPLY CHAIN RISK MANAGEMENT (SCRM) PROCESS

Federal ICT modernization efforts have increased reliance on the private sector and commercial off-the-shelf (COTS) products. These new products have increasingly complex, globalized, and dynamic supply chains, many of which include commercial suppliers that source from China at multiple points within a single supply chain. These supply chains change over time as companies develop new technologies and partner with new suppliers, and effective SCRM policies must be able to adapt as well. Nefarious actors linked to China have targeted the networks of private sector entities and private sector government contractors in order to obtain sensitive government information and to exploit vulnerabilities within federal information systems. Thus, weaknesses in the networks of industry partners pose a threat to the U.S. government and U.S. national security.

Defending against supply chain attacks by nefarious actors linked to China requires communication and collaboration with private sector actors. The National Institute of Standards and Technology (NIST) has been effective in partnering with the private sector to produce high-quality, implementable standards to improve supply chain security and cybersecurity of ICT systems, including the widely adopted NIST Cybersecurity Framework. Although NIST has been effective in these efforts, supply chain controls developed by NIST apply only to "high-impact" federal information systems.[4] Future work by NIST could include expanding supply chain standards to a broader range of federal information systems, including systems operated by private sector contractors.

Partnering with industry also means learning from experience with efforts such as the Bush-era Comprehensive National Cybersecurity Initiative (CNCI). The CNCI's effectiveness was limited by the classified nature of its deliberations and decisions, which prevented the U.S. Department of State and the National Cyber Security Center from engaging with outside organizations, including the private sector. Policymakers must empower rather than hinder the efforts of successful collaborative entities such as NIST and keep as much discussion of the supply chain threat as possible in the unclassified public sphere. These steps will ensure that new SCRM policies can be adaptive, be collaborative, and achieve buy-in from all relevant parties.

4 FIPS Publication 199 categorizes an information system as high impact as when "the loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals." In this case, "A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries." If any of the information on a federal information system is classified as high impact with respect to confidentiality, integrity, or availability, then the entire information system is considered high impact. See National Institute of Standards and Technology, *FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems* (Gaithersburg, MD: Computer Security Division, February 2004), http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

CENTRALIZE FEDERAL ICT SCRM EFFORTS

The U.S. government lacks a consistent, holistic SCRM approach. Additionally, most federal SCRM-related intelligence gathering activities are people based rather than technology based. This makes it difficult for federal SCRM programs to address the global threat comprehensively, or to scale as demand increases. The conflicting and confusing laws and regulations result in loopholes, duplication of effort, and inconsistently applied policies. Congress and the Executive Branch should encourage information sharing and the consolidation of federal SCRM leadership to optimize collection and dissemination efforts. Centralized leadership for SCRM would need to be resourced and staffed appropriately and tasked with vetting to a prescribed level the suppliers and value-added resellers of products entering the federal IT network.[5] The Office of Management and Budget (OMB) could, through modifications to Circular A-130,[6] assign centralized SCRM authority to the General Services Administration (GSA), the U.S. Department of Homeland Security (DHS), or another federal agency. This SCRM center would provide comprehensive and authoritative data and continuous monitoring, which would reduce the need for agency-specific SCRM and allow agencies to focus their efforts on particular configurations and implementation situations; how agencies use technology directly relates to how they apply risk mitigations. Last, such an office would need to function in the unclassified world, while at the same time having direct connections and reach-back authority into the classified environment to ensure it remains in alignment with known threats. As illustrated by the experience of the CNCI, the relationship should not be reversed and come entirely under classified control.

LINK FEDERAL REGULATIONS TO APPROPRIATIONS

Along with modifications to policy—such as Circular A-130—Congress should tie policy revisions to a funding strategy that ensures federal agencies take action in ways that are auditable. One recommendation is to expand the Wolf Provision, or Section 515 of the Consolidated and Further Continuing Appropriations Act, to apply to all federal agencies and entities. A near-term opportunity is to tie the SCRM requirements of this regulation to agency funding for the Modernizing Government Technology Act of 2017 in ways that require a SCRM program review for new ICT investments and modernization efforts. One improvement to the provision would be to require agencies to annually present (1) information about their established SCRM program, (2) the activities that have taken place within that program, and (3) the mitigations used. These annual reports will help build a best practices library for all federal government entities, increasing information sharing and awareness of evolving risks. The current reporting is compliance oriented and does nothing to share information or increase the security posture of federal ICT networks.

PROMOTE SUPPLY CHAIN TRANSPARENCY AND PARTNERSHIP WITH INDUSTRY

Supply chain transparency increases the security of the federal ICT supply chain by enabling the federal government to source responsibly and securely, and by improving the government's ability to respond to, and reduce the impact of, cybersecurity incidents in an environment where supply chain attacks are ongoing. Directly in relation to the impact on national security, the federal government should promote the public listing—or at least the disclosure to the government customer—of federal ICT providers and primary or tier-one suppliers in line with actions already taken by companies such as Dell, Hewlett-Packard (HP), and Microsoft as part of their corporate responsibility efforts. The government should also push for transparency on the part of all suppliers within its own supply chain according to the level of risk management rigor required (not all programs and suppliers present the same level of risk and therefore this level of transparency may not be needed). This information does not always need to be publicly released, though audit measures should be in place to ensure the transparency exists. In taking these measures, policymakers should learn from previous supply chain transparency efforts, such as Section 1502 of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, which required some companies to document their suppliers of "conflict minerals" in order to decrease violence in the Democratic Republic of the Congo (DRC) by limiting U.S. procurement from actors fueling conflict in the DRC. By partnering with industry and sharing information, the government customers and industry will have increased awareness of risks present in multi-tiered supplier relationships, as well as potentially effective mitigations that are already in place.

5 A value-added reseller is a company that purchases products from a vendor (generally at a discount); adds additional features, services, or support to the existing product; and then resells the product as an "integrated" or "turn-key" solution.

6 Circular A-130 provides policy guidance to federal agencies on the governance of IT resources, including governance, acquisitions, records management, open data, workforce, security, and privacy. The circular established minimum requirements for federal information security and privacy programs and assigns responsibilities for the security of those systems.

CRAFT FORWARD-LOOKING POLICY

Increasingly, any ICT component's physical structure pales in importance compared with the firmware and software operating within in it. Future risks will involve software, cloud-based infrastructures, and hyper-converged products rather than hardware. A vendor's, supplier's, or manufacturer's business alliances, investment sources, and joint research and development (R&D) efforts are also sources of risk that are not always covered in traditional SCRM. Identifying these risks and addressing them creatively as part of the adaptive approach to supply chain risk management will be important to the success of federal policy efforts.

Chapter 1: U.S. Government ICT Supply Chains

The OMB's 2017 budget proposal allocated $89.9 billion for IT in fiscal year (FY) 2017.[7] In 2016, International Data Corporation's (IDC's) Government Insights and FedScoop jointly released a study claiming that the U.S. federal ICT market is "the largest single vertical market for IT in the U.S. today, representing about 8.6 percent of all IT spending in the U.S., followed by the banking industry, at 7.6 percent."[8] FedScoop released two rankings in connection with the study: the "Top 25 Enterprise IT Providers to Government" and the "Federal IT Top 100." The top 10 companies on each list are shown in **Table 1**. Despite the size of the U.S. federal ICT market, IDC's research indicates that over 50 percent of federal IT spending goes to the top 10 suppliers on the lists, making their supply chains worthy of particular scrutiny for potential risk access points. It should be noted that Intel ranks at number 11 on the "Top 25 Enterprise IT Providers to Government" list, and also serves as a provider of primary technology components to many of the other companies in the top 10, thus its inclusion in this report.

THE FEDERAL ICT ECOSYSTEM

IDC and FedScoop's "Top 25 Enterprise IT Providers to Government" list ranks major enterprise IT companies by their estimated government-only sales.[9] The list includes the largest manufacturers of federal ICT equipment, including leading providers of COTS products, such as HP, IBM, Dell, Cisco, Unisys, Microsoft, and Intel.

The second list, the "Federal IT Top 100," ranks integrators and solution providers on the basis of revenue from the sale of IT products and services to federal agencies.[10] This list includes key players in government ICT contracting—firms that provide, manage, and, in some cases, modify the products produced by firms on the enterprise providers list.

Table 1
Federal IT Spending Ranked by Provider, FY 2015

Ranking	Top 25 Enterprise IT Providers to Government	Federal IT Top 100
1	Hewlett-Packard	Lockheed Martin
2	IBM	National Security Technologies
3	Jeppesen Sanderson (Division of Boeing)	Leidos, Inc.
4	Dell	Battelle Memorial Institute
5	Computer Sciences Corporation[1]	Northrop Grumman
6	Cisco	SAIC
7	Boeing	UChicago Argonne
8	Deloitte Consulting	Harris
9	Unisys	Consolidated Nuclear Security
10	Microsoft	Raytheon

Note: These rankings are based on actual revenues generated from the sale of IT products and services during the federal government's FY 2015, not multiyear contract awards. IDC has removed non-IT spending that is often included in IT contracts (such as management, consulting, and energy costs).

1. On April 3, 2017, Computer Sciences Corporation merged with Hewlett-Packard Enterprise Services to create DXC Technology.

Sources: IDC Government Insights and FedScoop.

7 Phil Goldstein, "2017 Budget Boosts IT Spending to $89.9 Billion, Expands U.S. Digital Service," *FedTech*, February 9, 2016, https://fedtechmagazine.com/article/2016/02/2017-budget-boosts-it-spending-899-billion-expands-us-digital-service.

8 Wyatt Kash, "New Top 100 Rankings Reveals Which Firms Earn the Most from Federal IT Spending," FedScoop, June 24, 2016, https://www.fedscoop.com/federal-it-top-100-report-on-government-it-spending/.

9 "Top 25 Enterprise IT Providers to Government," FedScoop, August 30, 2017, https://www.fedscoop.com/federal-it-top-25/federal-it-top-25-full-list/.

10 "Federal IT Top 100 – Federally Focused IT Providers," FedScoop, August 30, 2017, https://www.fedscoop.com/federal-it-top-100/full-list/.

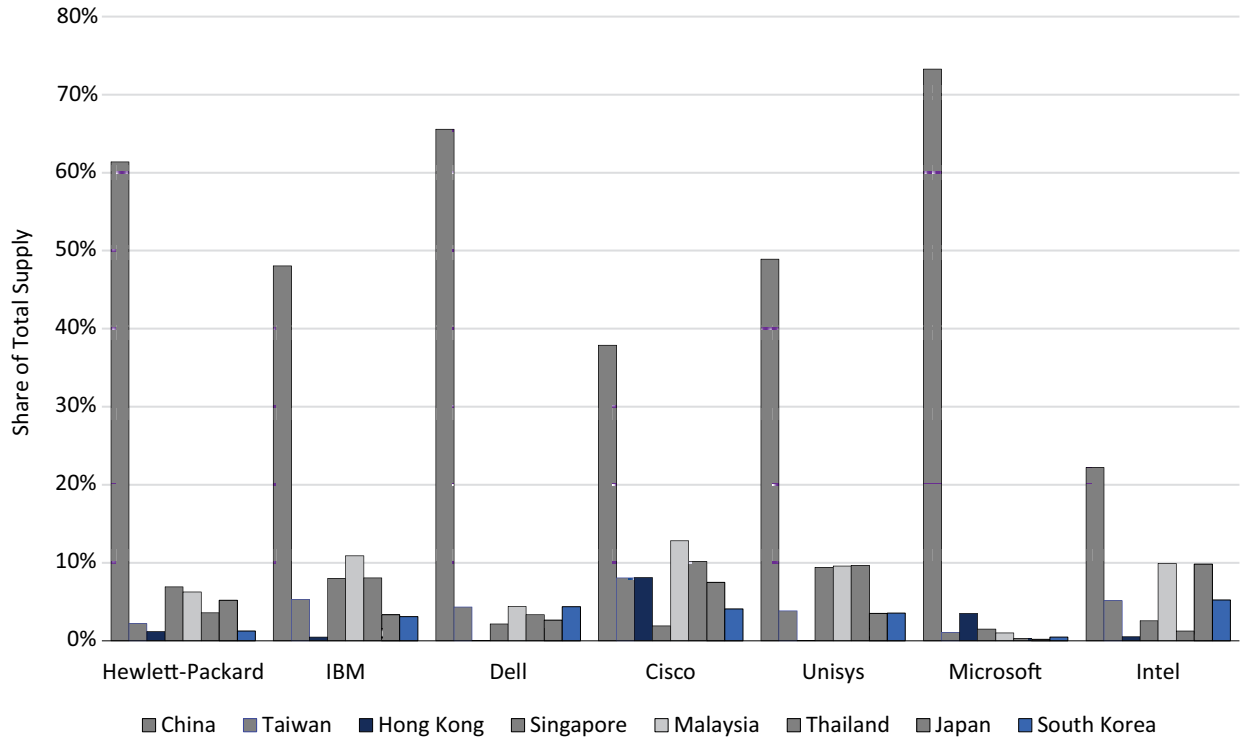
QUANTIFYING THE CHINA SUPPLIER NEXUS

In breaking down the supply chain implications for top companies on the enterprise providers list, this report focuses on seven manufacturers: HP, IBM, Dell, Cisco, Unisys, Microsoft, and Intel. These seven companies are some of the top IT providers to the U.S. government that are primarily IT manufacturers, and for which sufficient open source supply chain data exist. The nature of available open source information can make it difficult to separate data from a parent company from those of its subsidiaries; for example, data for Jeppesen Sanderson are tied to data for Boeing. The available data sets for Computer Sciences Corporation and Deloitte Consulting are too small to support firm conclusions. Focusing on these seven major IT manufacturers can illustrate the trends and challenges of supply chain risk analysis for commercial IT products. This is not to say these are the only companies with potential challenges in their supply chains, and it should be noted that none of these companies were approached as part of this report. Although each company conducts some level of due diligence on its supplier base, the complete records are not publicly available. Additional analysis of the aforementioned Jeppesen Sanderson, DXC Technology, and Deloitte, as well as other top federal enterprise IT providers such as AT&T, Abacus Technology, and Amazon Web Services, would provide a more comprehensive understanding of the federal ICT ecosystem.

Exhibit 1 provides transactional data culled from publicly available information for HP, IBM, Dell, Cisco, Unisys, Microsoft, and Intel. The graph shows the percentage of shipments originating in various countries between September 8, 2012, and September 7, 2017, for each company and its subsidiaries. These data provide a broader picture than U.S. trade data, as they include import and export data for other countries as well, including Bolivia, Chile, China, Colombia, Costa Rica, Ecuador, Mexico, Panama, Paraguay, Peru, Uruguay, and Venezuela. As the chart shows, China is the overwhelming source of products for these manufacturers. An average of 51 percent of shipments to these seven commercial IT manufacturers originate in China. Microsoft has the largest share of shipments originating in China, at 73 percent.

Exhibit 1

China Supply for Seven Leading Federal IT Providers, 2012–2017



Source: Panjiva.

Over 95 percent of all commercial electronics components and IT systems supporting U.S. federal IT networks are COTS, and China's role in this global supply network is significant. The supply chain for commercial IT is a global enterprise dominated by suppliers in East Asia.[11] In addition to Chinese firms, many companies headquartered in Taiwan and Singapore base their manufacturing operations primarily in China. China assembles most of the world's consumer and commercial electronic devices, produces parts such as flash cards, and dominates the world in volume of IT industrial capacity. A recent report from the Government Accountability Office (GAO) notes that China is the largest importer and exporter of IT hardware globally, as well as a key manufacturing location of workstations, notebook computers, routers and switches, fiber optic cabling, and printers.[12]

TRACING THE CHINA SUPPLIER NEXUS

Changing market dynamics and the increasing complexity of the commercial ICT supply chain have created additional challenges for supply chain risk management. During the transformation from raw materials to finished products, ICT components can transit several national borders. As one study showed, the elements that are eventually incorporated into an Apple iPod may be sourced from suppliers in the United States, Japan, Taiwan, and South Korea and assembled in plants in China run by Taiwanese corporations.[13] Assembled products may then pass through distribution centers in South and Central America to retail locations across the United States. This circuitous production path complicates the accuracy of trade data, as recent studies have shown, as well as the process of supplier management and supply chain tracing. Not only is it difficult to calculate the value added during each manufacturing step, but it is difficult to assess the risks associated with each new component supplier and contract manufacturer in the supply chain.

In addition, it is increasingly difficult for analysts to independently understand the nature of ICT supply chains. As little as 5–10 years ago, data from transactional information sources could trace ICT shipments from component producers in mainland China and Taiwan to manufacturing centers in North and South America. However, as the emerging middle class in China consumed more ICT technologies, China, Hong Kong, and Taiwan became favored locations for ICT firms' production facilities.[14] In China especially, government subsidies and policies requiring relocation in exchange for market access further encouraged multinationals to establish subsidiaries and joint ventures on the mainland. The establishment of multinational subsidiaries in East Asia has made independent open source supply chain analysis more difficult. Often the biggest supplier for many U.S. ICT companies, especially the larger ones, is their own East Asian subsidiary. For example, the largest supplier for Intel-Mexico, Intel-Colombia, and Intel-USA is Intel-Shanghai. Identifying the secondary and tertiary suppliers that contribute products and value early in the supply chain can be challenging due to the lack of transparent documentation and constantly changing business relationships. **Exhibit 2** provides an example of this phenomenon.

11 Danny Lam and David Jimenez, "US' IT Supply Chain Vulnerable to Chinese, Russian Threats," *The Hill*, July 9, 2017, http://thehill.com/blogs/pundits-blog/technology/341177-us-it-supply-chain-vulnerable-to-chinese-russian-threats.

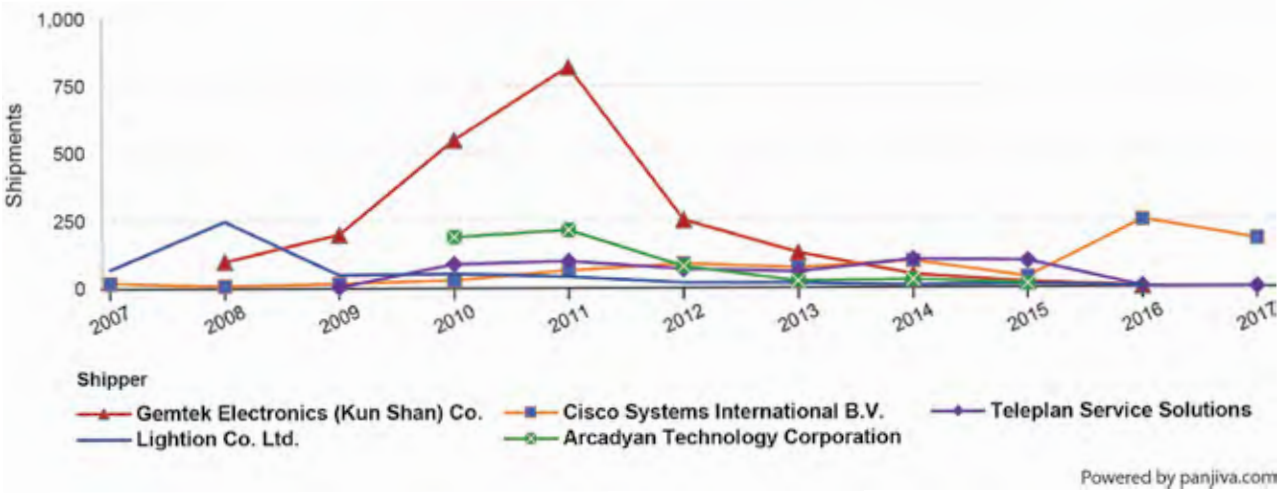
12 U.S. Government Accountability Office, "State Department Telecommunications: Information on Vendors and Cyber-Threat Nations" (GAO-17-688R State Department Telecommunications, July 27, 2017), https://www.gao.gov/assets/690/686197.pdf.

13 Greg Linden, Kenneth L. Kraemer, and Jason Dedrick, "Who Captures Value in a Global Innovation Network? The Case of Apple's iPod," *Communications of the ACM* 52, no. 3 (March 2009): 140–44, http://pcic.merage.uci.edu/papers/2008/whocapturesvalue.pdf.

14 Organisation for Economic Co-operation and Development (OECD), *OECD Science, Technology and Innovation Outlook 2016* (Paris: OECD Publishing, 2016), http://dx.doi.org/10.1787/sti_in_outlook-2016-en.

Exhibit 2

Annual Shipments by Suppliers to Cisco Systems, 2007–2017



Source: Panjiva.

Exhibit 2 shows the year-to-year shift in Cisco's U.S. import registered supplier data, as shipments from Gemtek Electronics (Kun Shan) Co. Ltd. (China), Arcadyan Technology Corporation (Taiwan), and Lightion Co. Ltd. (Hong Kong) gradually disappear from the data set and are replaced by shipments from Cisco Systems International B.V., a subsidiary based in the Netherlands that appears to manage Cisco's international shipments. This trend effectively masks the deeper levels of Cisco's supply chain, making it less clear which East Asian companies are serving as third- and fourth-tier suppliers.

A similar pattern is evident among the other top enterprise IT providers to the federal government. HP's top two suppliers of China-origin goods are its own subsidiaries in Singapore and Mexico. Unisys's primary shipper of China-origin products is Unisys C O Exel, which began shipping from China to Unisys subsidiaries in Mexico and Colombia around 2012. For Intel, Microsoft, Cisco, Boeing, and IBM, the top supplier of China-origin items is the company itself.

The practice of sourcing primarily from foreign subsidiaries can make it more difficult to determine the primary component suppliers in a supply chain, and this lack of transparency is itself an added source of risk. This is because for SCRM, both the location of the production and the entity in control of that production are important factors in assessing risk. Risks associated with location and control of production exist along a spectrum, and can be aggravated or mitigated by other factors. Production by a Chinese state-owned enterprise (SOE) based in China presents greater risk to the federal ICT supply chain than production by a Singaporean firm based in China, yet both present more risk than a Singaporean firm based in Singapore. This is because production based in sensitive countries or in countries known for counterfeiting and intellectual property (IP) violations poses heightened risk regardless of who does the manufacturing. Due to reliance on foreign legal, political, and financial systems and labor markets, as well as the infrastructure of a foreign nation, foreign subsidiaries may be at greater risk of penetration by nefarious actors than domestic subsidiaries and a company's recourse in the event of penetration may be more limited. In China in particular, companies involved in trade disputes or corporate litigation can encounter difficulties obtaining records or serving subpoenas that would allow prosecution, and must prove they have taken steps to properly safeguard trade secrets in order to successfully sue.[15]

15 Del Quentin Wilber, "Stealing White: How a Corporate Spy Swiped Plans for DuPont's Billion-Dollar Color Formula," Bloomberg, February 4, 2016, https://www.bloomberg.com/features/2016-stealing-dupont-white/.

The entity in control of production also factors into the analysis. A parent company has most control over location security, staff hiring, manufacturing, and quality control practices at domestic subsidiaries. Depending on a company's corporate culture and internal controls, that same company may have more control at a foreign subsidiary than it would at a foreign third-party manufacturer. Apple, for instance, has instituted strict controls at its production sites in China in an effort to secure its supply chain and protect its IP.[16] However, the foreign subsidiary may still be subject to foreign regulations or influence in ways that increase risk related to a company and its products.

16 William Turton, "Leaked Recording: Inside Apple's Global War on Leakers," *The Outline*, June 20, 2017, https://theoutline.com/post/1766/leaked-recording-inside-apple-s-global-war-on-leakers.

Chapter 2: SCRM Laws, Regulations, and Other Requirements

Supply chain risk management is an important component of a comprehensive cybersecurity mission, but it also has a role in market research, acquisitions, and procurement, as well as broader programmatic activities such as program lifecycle planning. A challenge facing federal SCRM efforts is that federal government laws and policies do not address risk management comprehensively. Rather, as the following sections will show, SCRM of federal ICT systems has been divided in multiple ways—among federal information systems and other initiatives designed to protect critical infrastructure or high-value assets and among national security systems (NSS) as a subset of federal information systems.

FEDERAL INFORMATION SYSTEMS AND NIST

The OMB has purview over federal information systems "used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency."[17] NIST creates standards and guidelines for these systems. NIST is not a regulatory agency; rather, it develops security standards and guidelines through a comprehensive public review process. For many products, this process involves three cycles of public vetting, during which comments on draft publications are solicited from individuals and organizations in the public and private sectors.[18] NIST's outreach efforts encourage feedback and discussion, particularly from owners, operators, and administrators of the information systems for which NIST sets standards. This process aims to ensure that the guidelines are both technically correct and implementable.

In 2002, Congress passed the Federal Information Security Management Act (FISMA), which required NIST to develop security standards and guidelines to protect federal information systems and allowed the OMB to make NIST standards compulsory and binding.[19] NIST's FISMA Implementation Project was established in 2003 to produce the required security standards and guidelines for federal information systems; its publications include Federal Information Processing Standards (FIPS) 199, FIPS 200, and the NIST Special Publications (NIST SP) 800 series.

Neither FIPS 199 (2004) nor FIPS 200 (2006) mention supply chain issues. FIPS 199 focuses on categorization, creating the requirement to rate information systems as low, moderate, or high impact in terms of confidentiality, integrity, and availability.[20] FIPS 200 sets some minimum security requirements in the areas of access control, awareness and training, configuration management, media protection, personnel security, resource allocation, and licensing policy, among others. FIPS 200 also introduced the concept that risk management includes "continuous" or "ongoing" monitoring of the security state of the information system.[21]

The FIPS 199 categorizations and policies are used to determine which systems are subject to enhanced cybersecurity measures and SCRM requirements, but the FIPS standards do not require SCRM of those systems, or specify the scope or extent of supplier due diligence that should be used in evaluating products, services, or suppliers of those systems. The FIPS 200 controls are designed to mitigate threats posed by individuals who are improperly trained or credentialed, and to avoid resource management errors that may result in an improperly disposed hard drive or an improperly used or licensed software program. They are not designed to mitigate risk posed by ICT products that may have been compromised during the manufacturing, programming, or deployment process. This separation is intentional. Supplemental information released with FIPS 200 in March 2006 explained that during the review

17 "Circular No. A-130: Managing Information as a Strategic Resource," Office of Management and Budget, July 28, 2016, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf.

18 "FAQs: General Questions, National Institute of Standards and Technology," Computer Security Resource Center, updated October 18, 2017, http://csrc.nist.gov/groups/SMA/fisma/faqs.html.

19 This means that standards created under the authority of Sections 20(a) and 20(b) of the National Institute of Standards and Technology Act 15 U.S.C. 278g–3(a) were mandatory.

20 National Institute of Standards and Technology, *FIPS PUB 199*.

21 National Institute of Standards and Technology, *FIPS PUB 200: Minimum Security Requirements for Federal Information and Information Systems* (Gaithersburg, MD: Computer Security Division, March 2006), http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf.

process NIST had received comments suggesting "additions and changes to the standard concerning risk management procedures, audit controls, baseline security controls, and risks introduced by new technologies," all of which could be considered SCRM-related. NIST's response to this comment indicated that these elements were best addressed in forthcoming NIST SP 800-53, and ultimately aggregated from across all NIST SPs in SP 800-161, rather than updated in the FIPS 199 and 200 series.[22] The result of this decision is that while FIPS 199 and 200 controls are legally mandated, the SCRM-related controls in NIST SPs remain merely guidance. A stronger legal or regulatory requirement relating to SCRM could help bridge this gap. That said, it is not—nor should it be—the role of NIST to enforce stronger legal or regulatory requirements, as this would severely diminish NIST's value as convening entity.

NATIONAL SECURITY SYSTEMS AND THE CNSS

Policies for NSS are controlled by the Committee on National Security Systems (CNSS). The CNSS is an interagency body chaired by the Department of Defense (DoD) and the U.S. military, with membership from the intelligence community, the DHS, the Department of Justice, and other entities. The CNSS was formed in 2001 by Executive Order 13231; it evolved from the National Security Telecommunications and Information Systems Security Committee, which had been created in 1990. The executive agency for the CNSS is the National Security Agency (NSA).

The Federal Information Security Management Act of 2002 defines NSS as follows:

> *(2)(A) The term "national security system" means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—*
>
> *(i) the function, operation, or use of which—*
>
> *(I) involves intelligence activities;*
>
> *(II) involves cryptologic activities related to national security;*
>
> *(III) involves command and control of military forces;*
>
> *(IV) involves equipment that is an integral part of a weapon or weapons system; or*
>
> *(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or*
>
> *(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.*
>
> *(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).*[23]

Or, as the DoD explains, an NSS is—

> *A telecommunications or information system operated by the Federal Government that involves intelligence activities; cryptologic activities related to national security; command and control of military forces; equipment that is an integral part of a weapon or weapons system; or that is critical to the direct fulfillment of military or intelligence missions.*[24]

22 National Institute of Standards and Technology, *Announcing Approval of Federal Information Processing Standard (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems* (Gaithersburg, MD: Computer Security Division, March 2006), https://www.federalregister.gov/documents/2006/03/31/E6-4720/announcing-approval-of-federal-information-processing-standard-fips-200-minimum-security.

23 FISMA, Pub. L. No. 107-347, Title III (December 17, 2002).

24 Inspector General, Department of Defense, "DoD's Policies, Procedures, and Practices for Information Security Management of Covered Systems" (Report No. DODIG-2016-123, Department of Defense, Alexandria, VA, August 15, 2016), http://www.dodig.mil/pubs/documents/DODIG-2016-123.pdf.

Thus, NSS encompass more than military or intelligence systems, or various levels of classified information.[25] For example, the Department of Energy has NSS by virtue of its mission to maintain the nuclear weapons stockpile. Similarly, other agencies including the Departments of Energy, State, Treasury, and Justice all have roles in intelligence, a mission not limited to agencies such as the Central Intelligence Agency and the DoD.

Although the CNSS was established to develop operating policies, procedures, guidelines, instructions, and standards for NSS, FISMA specifically grants the Secretary of Defense and the Director of Central Intelligence separate, individual authority over their own systems. As stated in a 2002 House Committee on Government Reform report, "This guidance is not to govern such systems, but rather to ensure that agencies receive consistent guidance on the identification of systems that should be governed by national security system requirements."[26]

EXECUTIVE BRANCH AND SCRM

Congress is not alone in its ability to influence NIST and federal ICT policy; actions by the Executive Branch have advanced the ICT and SCRM agenda in important ways.

The Comprehensive National Cybersecurity Initiative was established by President George W. Bush in January 2008 through National Security Presidential Directive 54/Homeland Security Presidential Directive 23 and expired under President Barack Obama.[27] The directive established the foundation for current DoD policy on cybersecurity issues and provided the initial impetus to the DoD's SCRM efforts by including funding for pilot programs and reports on results, elements of which were the basis for subsequent comprehensive enterprise SCRM programs. The directive called for the Secretaries of Defense and Homeland Security, in coordination with the Secretaries of the Treasury, Energy, and Commerce; the Attorney General; the Director of National Intelligence; and the Administrator of General Services, to develop a strategy and implementation plan to, among other issues, "better manage and mitigate supply chain vulnerabilities," including specific recommendations for the federal government and defense acquisition process. The CNCI itself aimed to reduce federal ICT vulnerabilities and prevent intrusions; strengthen supply chain security; and enhance research, development, education, and investment in key technologies. The DHS and DoD were the lead agencies for the SCRM initiative, but the directive and its related activities remained classified. A March 2010 report on the initiative by the Government Accountability Office noted that the classification level hindered efforts by the Department of State and the National Cyber Security Center to engage outside organizations, including the private sector.[28]

In March 2010, the DoD issued DoD Directive-Type Memorandum 09-016–SCRM to Improve the Integrity of Components Used in DoD Systems. The directive defined SCRM and supply chain risk, and stated that supply chain risk shall be addressed early and across the entire system lifecycle through a defense-in-breadth approach to managing the risks to the integrity of ICT within covered systems.

25 Further details on the connection between NSS and classified information can be found in National Security Agency, *CNSSI No. 1253: Security Categorization and Control Selection for National Security Systems* (Ft. Meade, MD: CNSS Secretariat, March 2014), http://www.dss.mil/documents/CNSSI_No1253.pdf; and National Security Agency, *CNSSI No. 1253 Attachment 5: Classified Information Overlay* (Ft. Meade, MD: CNSS Secretariat, May 2014), http://cryptome.org/2014/05/cnss-classified-info-overlay.pdf.

26 National Institute of Standards and Technology, *NIST Special Publication 800-59: Guideline for Identifying an Information System as a National Security System* (Gaithersburg, MD: Computer Security Division, August 2003), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-59.pdf; U.S. House of Representatives, "Report of the Committee on Government Reform" (Report 107-787, November 14, 2002), 85, quoted in NIST Special Publication 800-59.

27 "National Security Presidential Directive/NSPD-54 and Homeland Security Presidential Directive/HSPD-23," The White House, (Washington, DC, January 8, 2008, https://www.georgewbushlibrary.smu.edu/~/media/GWBL/Files/Digitized%20Content/2014-0390-F/t030-021-012-nspd54-1-20140390f.ashx.

28 U.S. Government Accountability Office, "Cybersecurity: Progress Made by Challenges Remain in Devining and Coordinating the Comprehensive National Initiative" (GAO-10-338, Washington, DC, March 2010), http://www.gao.gov/new.items/d10338.pdf.

Directive-Type Memorandum 09-016 was subsumed in November 2012 by DoD Instruction 5200.44, which was modified by Change 1 in August 2016.[29] The 2012 Instruction considers National Security Presidential Directive 54/Homeland Security Presidential Directive 23 the basis for the directive's SCRM implementation strategy, along with the following references:

- National Security Presidential Directive 54/Homeland Security Presidential Directive 23, "Cybersecurity Policy," January 8, 2008
- Section 806 of Public Law 111-383, "The National Defense Authorization Act for Fiscal Year 2011," January 7, 2011
- DoD Directive 5000.01, "The Defense Acquisition System," May 12, 2003
- DoD Instruction 5000.02, "Operation of the Defense Acquisition System," December 8, 2008 (updated January 7, 2015)
- DoD Instruction 8500.01, "Cybersecurity," March 14, 2014 (from DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002)
- Committee on National Security Systems Directive No. 505, "Supply Chain Risk Management (SCRM)," March 7, 2012[30]

Military and intelligence systems are a subset of NSS, rather than the other way around, and DoD SCRM policies have largely been developed by the DoD itself, or by the DoD in concert with other members of the CNSS.

In 2013, President Obama's Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," provided an influential but unanticipated boost to SCRM policy. The executive order focused on improving the cybersecurity of "Section 9 entities," or "critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."[31] The order does not mention supply chain or SCRM, but it tasks NIST with creating "a framework to reduce cyber risks to critical infrastructure," including "a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks." This framework would become the NIST Cybersecurity Framework (NIST CSF).

The NIST CSF, published in February 2014, created the Identify, Protect, Detect, Respond, and Recover framework now ubiquitous throughout federal discussions of cybersecurity.[32] Supply chain issues make a brief appearance in the Business Environment category of the Identify section of the framework, which instructs organizations to identify their role in the supply chain. The framework highlights NIST SP 800-53 Rev. 4 as an informative reference for this subcategory. Other SCRM developments continued gradually from previous lines of effort, as when a revision to NIST SP 800-37, released in June 2014, briefly mentioned SCRM with respect to external providers of ICT products.[33] The NIST CSF now underpins much of the discussion surrounding federal ICT cybersecurity, and thus SCRM, for federal ICT networks. Despite the framework's origins as an effort focused on critical infrastructure, it has been adopted by numerous federal organizations.

---

29 Department of Defense, "Department of Defense Instruction 5200.44" (August 25, 2016), https://www.hsdl.org/?abstract&did=795012.

30 National Security Agency, *CNSSD No. 505: Supply Chain Risk Management* (Ft. Meade, MD: CNSS Secretariat, March 7, 2012), https://info.publicintelligence.net/CNSS-SupplyChainRisk.pdf.

31 The White House, "Executive Order–Improving Critical Infrastructure Cybersecurity" (Office of the Press Secretary, Washington, DC, February 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

32 National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (February 12, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

33 National Institute of Standards and Technology, *NIST Special Publication 800-37 Revision 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Live Cycle Approach* (Gaithersburg, MD: Computer Security Division, February 2010), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf.

CONGRESSIONAL ACTION AND SCRM

The Federal Information Technology Acquisition Reform Act (FITARA), FISMA, and the Cybersecurity Enhancement Act currently delineate the bounds of debate surrounding federal ICT risk management.

Federal Information Technology Acquisition Reform Act

Although introduced in 2013, the final version of FITARA did not become law until late 2014, when it passed as part of the FY 2015 National Defense Authorization Act.[34] FITARA had seven primary focus areas:

1. Enhancing the authority of the chief information officer
2. Enhancing transparency and improved risk management in IT investments
3. Requiring savings through IT portfolio review
4. Expanding the training and use of IT cadres
5. Consolidating federal data centers
6. Maximizing the benefit of the Federal Strategic Sourcing Initiative
7. Expanding government-wide software purchasing programs

FITARA tasked the OMB with implementing a process for ICT portfolio review and reviewing ICT acquisition staffing demands. FITARA was passed with fiscal concerns in mind and is commonly understood as an attempt to properly plan and manage incredibly expensive IT acquisitions. Congress views FITARA primarily as a fiscal oversight initiative designed to prevent costly spending, rather than as a security policy. Conversations between Interos leadership and congressional offices revealed Congress is reluctant to securitize FITARA by adding SCRM elements to the policy, such as requiring baseline vendor vetting prior to approving acquisitions. However, like previous policy efforts, FITARA has affected supply chain issues indirectly.

FITARA helps federal chief information officers increase visibility over their ICT infrastructure, potentially reducing vulnerabilities due to lack of oversight and transparency of what systems exist and therefore need some aspect of security. Perhaps somewhat paradoxically, however, FITARA's focus on portfolio review encourages agencies to identify aging infrastructure elements and consolidate them through new technologies. Portfolio review encourages modernization, and modernization introduces new COTS products into federal ICT systems. Due to the nature of global ICT supply chains, most new products that will enter federal ICT systems will include components originating in China or produced by Chinese firms. The use of COTS presents some challenges, given the confidentiality, integrity, and accessibility requirements for federal systems. In September 2017, FedScoop announced the results of a survey of 200 federal IT executives conducted by Unisys Corporation and the research company Market Connections. Fifty-nine percent of survey respondents said IT modernization efforts have increased the cybersecurity challenges they face.[35]

A lack of compliance with FITARA can be an indicator of cybersecurity vulnerabilities resulting from aging and poorly maintained ICT infrastructure, including vulnerabilities originating from supply chain risks. More important, a chief information officer's limited oversight of their federal IT systems creates potential gaps in security. This said, compliance with FITARA does not itself directly equal achieving comprehensive cybersecurity or oversight of a federal ICT supply chain.

The Modernizing Government Technology Act could place similar pressure on federal agencies. The bill was introduced by U.S. Representative Will Hurd (R-TX), chairman of the House Information Technology Subcommittee, in September 2016.[36] The act creates a $500 million central modernization fund that agencies can

34 Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015, H.R. 3979, 113th Cong. (2013–2014), https://www.congress.gov/bill/113th-congress/house-bill/3979.

35 Carten Cordell, "IT Modernization Efforts Increase Cybersecurity Challenges, Survey Says," FedScoop, September 6, 2017, https://www.fedscoop.com/survey-modernization-efforts-increasing-cybersecurity-challenges/.

36 Modernizing Government Technology Act of 2016, H.R. 6004, 114th Cong. (2015–2016), https://www.congress.gov/bill/114th-congress/house-bill/6004.

borrow against to update aging IT systems.[37] The act also creates working IT capital funds that allow agencies to retain savings achieved from ongoing modernization efforts, provided they are used for future modernization projects. The bill was amended to the Senate version of the National Defense Authorization Act, which was passed by Congress in November 2017 and signed into law on December 12, 2017.[38]

The Modernizing Government Technology Act seems to presume that legacy equipment and systems are the sole source of risk, and that this risk can be mitigated through modernization. But modernization will actually increase risk if newly adopted technologies are not assessed appropriately before being integrated into federal IT networks. The bill establishes responsibilities and financial rewards to the agencies for modernizing their IT infrastructure and names the OMB and GSA as permanent members of a supervisory board, but it does not require any measure of supply chain security as part of modernization efforts. In the memorandum on "Implementation of the Modernizing Government Technology Act" signed by OMB Director Mick Mulvaney on February 27, 2018, there are multiple pages of guidelines for the execution of the program, but no requirement for SCRM as part of an agency's request for modernizing funds.[39]

As federal agencies face additional pressure from efforts like FITARA and the Modernizing Government Technology Act, the need for robust ICT SCRM leadership as well as an appropriately resourced capability becomes ever more important, affecting the ICT products agencies acquire, how and at what speed they acquire them, the suppliers they use, and the eventual quality and security over the product lifecycle.[40]

Federal Information Security Modernization Act and Circular A-130

FISMA sought to centralize federal cybersecurity management with the DHS, retaining the OMB's authority over policies for federal information systems but charging the DHS with the implementation of those policies. The bill retained the prerogatives of the Secretary of Defense and the Director of National Intelligence for their own systems. Although FISMA 2014 required continuous cybersecurity monitoring, sparking the DHS-led Continuous Diagnostics and Mitigation program, FISMA did not address SCRM specifically, creating yet another gap in federal laws and regulations.

The passage of FISMA 2014 also tasked NIST with continuing its work to protect federal information systems. In April 2015, NIST released SP 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," the most detailed NIST contribution to the SCRM discussion since the creation of Control SA-12 in 2010. NIST SP 800-161 adopted the definition of risk from FIPS 200 to establish a definition for ICT supply chain risk and built on NIST SP 800-53 Rev. 4 and NIST Interagency Report 7622, *National Supply Chain Risk Management Practices for Federal Information Systems*, to enhance the overlay of ICT-specific SCRM controls.[41]

The OMB incorporated the new FISMA requirements and NIST controls into active policy. In support of FISMA 2014, the OMB issued Circular A-123 and revised Circular A-130 in July 2016. Circular A-123 broadened the scope of risk management beyond fiscal compliance and required federal organizations to establish an enterprise risk management capability, of which A-130 and SCRM are key components.[42] The release of a revised Circular A-130

37 National Defense Authorization Act for Fiscal Year 2018, H.R. 2810, 115th Cong. (2017–2018), https://www.congress.gov/bill/115th-congress/house-bill/2810.

38 Jason Miller, "In the End, Senate Lets the MGT Act in the Defense Bill," *Federal News Radio*, September 19, 2017, https://federalnewsradio.com/legislation/2017/09/in-the-end-senate-lets-the-mgt-act-in-the-defense-bill/; Carten Cordell, "Trump Signs Modernizing Government Technology Act into Law," FedScoop, December 12, 2017, https://www.fedscoop.com/trump-signs-mgt-act-law/.

39 The White House, "M-18-12, OMB Memorandum, Implementation of the Modernizing Government Technology Act" (Washington, DC: Office of Management and Budget, February 27, 2018), https://www.whitehouse.gov/wp-content/uploads/2017/11/M-18-12.pdf

40 "The Importance of SCRM's Role in Connection to FITARA," Interos Solutions, February 9, 2015, https://interosblog.wordpress.com/2015/02/09/the-importance-of-scrms-role-in-connection-to-fitara/.

41 National Institute of Standards and Technology, *NIST Special Publication 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (Gaithersburg, MD: Computer Security Division, April 2015), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf.

42 KMPG International, "A-123 Aims to Strengthen Government with Enterprise Risk Management," Government Executive, January 5, 2017. http://www.govexec.com/govexec-sponsored/2017/01/-123-aims-strengthen-government-enterprise-risk-management/134386/; The White House, "M-16-17, OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control" (Washington, DC: Office of Management and Budget, July 15, 2016), https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m-16-17.pdf.

was key, as it had not been updated since 2000.[43] The circular expanded on risk management issues and included specific supply chain security language. Perhaps most important, the circular requires agencies to implement security policies issued by the OMB, including standards and guidelines contained in NIST products, and formally establishes a shift from three-year review and authorizations of compliance activities to continuous monitoring of those activities. Appendix I of the circular details general requirements, implementation of FITARA, and SCRM principles.[44] The circular requires agencies to develop SCRM plans as described in NIST SP 800-161 and to satisfy the information security requirements in FIPS 200 and the security control baselines in NIST SP 800-53. It should be noted that as of the writing of this report, there has been no known audit to ensure federal agencies have impactful SCRM programs in place, nor is there policy that mandates a government-wide national supply chain risk management strategy.

Cybersecurity Enhancement Act

As part of the implementation of President Obama's Executive Order 13636, Congress modified NIST's mission in the Cybersecurity Enhancement Act of 2014, to have NIST continue work on the CSF and expanded the use of the CSF to owners and operators of critical infrastructure.[45]

This call for owners and operators of critical infrastructure to take NIST's work into account appears to be part of a broader move toward consolidating parts of the federal ICT policy framework. DoD Instruction 8500.01, issued in March 2014, required the DoD to implement system security controls designed by NIST, but it is DoD Instruction 5200.44, Change 1, effective August 2016, that explicitly adds NIST SP 800-161 as a basis for the implementation of the DoD SCRM strategy. Similarly, the CNSS released a revision of CNSS Directive 505, "Supply Chain Risk Management," in August 2017, replacing the directive published in March 2012.[46] The new directive makes explicit connections between the CNSS and NIST, explaining that the CNSS adopts NIST standards where applicable and publishes additional guidelines in instances where NIST does not sufficiently address the needs of NSS.

A new revision of the CSF was released for comment in January 2017, providing new details on managing cyber supply chain risks, clarifying key terms, and introducing measurement methods for cybersecurity. It also includes references to SCRM across all five components of the framework.[47] Increasingly integrating SCRM into federal risk management efforts is important to successfully managing the ICT modernization efforts envisioned in legislation like FITARA, but there remains no centralized leadership for federal SCRM efforts. Additionally, existing regulations and requirements do not adequately address the risk posed by COTS products, or risks related to ICT products linked to China or other state actors that may pose a threat to the United States.

43 The White House, "M-16-17."

44 Jason Miller, "OMB Initiates Cyber Marathon with Long-Awaited Policy Update," *Federal News Radio*, October 21, 2015, https://federalnewsradio.com/omb/2015/10/omb-initiates-cyber-marathon-long-awaited-policy-update/.

45 Cybersecurity Enhancement Act of 2014, S. 1353, 113th Cong. (2013–2014), https://www.congress.gov/bill/113th-congress/senate-bill/1353/text; "NIST Releases Update to Cybersecurity Framework," National Institute of Standards and Technology, January 10, 2017, https://www.nist.gov/news-events/news/2017/01/nist-releases-update-cybersecurity-framework.

46 National Security Agency, *CNSSD No. 505: Supply Chain Risk Management* (Ft. Meade, MD: CNSS Secretariat, July 26, 2012), https://1yxsm73j7aop3quc9y5ifaw3-wpengine.netdna-ssl.com/wp-content/uploads/2017/08/CNSSD_505_Final2-Published-08-01-2017.pdf.

47 "NIST Releases Update," National Institute of Standards and Technology.

Chapter 3: Supply Chain Analysis of Federal ICT Manufacturers

As previously stated, this study uses a comprehensive definition of "U.S. government ICT supply chains" that includes (1) primary suppliers, (2) tiers of suppliers that support prime suppliers by providing products and services, and (3) any entities linked to those tiered suppliers through commercial, financial, or other relevant relationships. The reason for this, as outlined below, is that the greatest risks are often unknown and driven directly by the location of the multiple tiers of suppliers and the nature of their third-party affiliations.

SUPPLIER LOCATION

No laws or regulations mandate that federal IT suppliers provide multi-tier transparency regarding their supply chains; however, HP, Dell, and Microsoft have embraced industry transparency principles in a way that allows some insight into their first-tier suppliers. All three publish lists of their primary suppliers, a practice that is not standard across the industry.[48] The lists are not constructed identically, so the data require some manipulation before they can be analyzed. Dell provides site addresses for all of its tier-one suppliers; HP provides site addresses for its final assembly suppliers but not for its commodity and component suppliers; and Microsoft provides a list of the names of its top 100 suppliers.[49]

For this paper, Interos analyzed the publicly reported supplier networks of HP, Dell, and Microsoft. Of the 344 identified suppliers for HP, Dell, and Microsoft, it was possible to identify a site address for 212. The 132 suppliers for which a site address could not be identified were categorized according to the location of their corporate headquarters. As expected, HP, Dell, and Microsoft source from the same companies; at times from the same company at the same site. As an example, all three source from Pegatron Corporation. Dell identified two site addresses from which it does business with Pegatron—one in Taoyuan City, Taiwan, and one in Jiangsu, China. HP also reported sourcing from the Jiangsu site. Because Microsoft reported sourcing from Pegatron, but did not identify a site, Microsoft was categorized as sourcing from Pegatron's headquarters in Taipei, Taiwan. Thus, the combined supplier list includes three entries for Pegatron: one for Taoyuan City, Taiwan; one for Jiangsu, China; and one for the Taipei, Taiwan headquarters. Using this categorization system, the unified suppliers list identifies 39 percent of suppliers to these three companies as located in China, 15 percent located in Taiwan, 13 percent located in the United States, and 8 percent located in Japan.

The links to China are more numerous than these data suggest, because a number of companies were categorized only by the location of their company headquarters. For the 132 companies for which a site address could not be conclusively determined, 87 were headquartered in Taiwan, the United States, or Japan. The unified supplier list categorizes these 132 suppliers only by the location of their headquarters, not by any supplier sites that may be elsewhere, yet it is common for companies headquartered in Taiwan, the United States, Japan, and other countries to base their production facilities in China. It is likely that a significant portion of these companies have operations in China, making China's influence on these supply chains larger than it appears at first glance.

SUPPLIER FINANCING AND INFLUENCE

Financial links to suspect entities, including state-owned or substantially state-controlled enterprises, are also important for SCRM, as they indicate potential vectors for nefarious influence. Previous reports have raised concerns about the connections between Intel, HP, Dell, IBM, Cisco, Microsoft, and Chinese entities such as

48 Apple follows similar transparency policies. Apple is a not a top 10 provider of enterprise ICT to the U.S. federal government, however, so its data were not included in this analysis.

49 Nick Wingfield and Charles Duhigg, "Apple Lists Its Suppliers for 1st Time," The New York Times, January 13, 2012, http://www.nytimes.com/2012/01/14/technology/apple-releases-list-of-its-suppliers-for-the-first-time.html; "HP Suppliers," Hewlett-Packard, http://h20195.www2.hp.com/V2/GetPDF.aspx/c03728062.pdf; "Our Suppliers," Dell, About Dell, Corporate Social Responsibility, Supply Chain, http://www.dell.com/learn/us/en/uscorp1/cr-social-responsibility; "Microsoft Top 100 Production Suppliers," Microsoft, http://download.microsoft.com/download/0/1/4/014D812D-B2E3-43A0-A89A-16E3C7CD46EE/Microsoft_Top_100_Production_Suppliers_2016.pdf.

Tsinghua Holdings, Inspur Group, Beijing Teamsun Technology, and the China Electronics Technology Group Corporation (CETC).[50] In the analysis of suppliers for HP, Dell, and Microsoft, 28 suppliers (that accounted for 52 supplier site locations) were identified as presenting some level of risk owing to their connections to Chinese state-owned entities. **Table 2** includes information on several of these entities of concern. Risk can be present in the nature of the government's relationship with an entity: "state-controlled" entities listed below function in some ways as part of official government or military institutions; "state-owned" entities have significant financial ownership or control by the state; "state-influenced" entities may have other, less formal, ties to a government, such as strategic partnerships or leadership connections; and "defense suppliers" provide services or products to a state's government, military, or security services.

For this report, Interos complied a listing of entities, their potential risk based on the relation to the Chinese government, and the publicly available sources this information was garnered from. Further research would need to be completed to truly understand the comprehensive risk these entities may pose to U.S. ICT supply chains.

Table 2
Examples of Federal ICT Suppliers Connected to Entities of Concern

Entity Name	Risk	Details	Source
Beijing Teamsun Technology	Defense supplier	Partnership with IBM.	Various.
BOE Global	State-owned	Supplies display/liquid crystal display to Dell.	15.24 percent owned by Beijing State-Owned Assets Supervision and Administration.
China Electronics Technology Group Corporation (CETC)	State-controlled Defense supplier	A network of former military labs that operates both commercial and military technology businesses. Strategic partnerships with Microsoft and IBM.	State-owned company according to Dow Jones.
Chinese Academy of Sciences (CAS)	State-controlled	Connections to Chinese military, nuclear, and cyberespionage programs. Often appears as an investor or partner of other Dell, HP, or Microsoft suppliers.	Various.
Huawei	National champion	Cyberespionage risk.	U.S. House Permanent Select Committee on Intelligence Investigative Report.
Inspur Group	Defense supplier	Joint ventures and partnerships with Cisco, Intel, and IBM.	Various.
Legend Capital/ Holdings	State-controlled	Asset management arm of the CAS, and the owner of Lenovo. Occasionally appears as an investor or partner of other Dell, HP, or Microsoft suppliers. Part of a consortium that acquired Lexmark in 2016.	Various.
Lenovo	State-owned	Cyberespionage risk.	29.10 percent owned by Legend Holdings Corp.
Lexmark	State-influenced	Acquired in April 2016 by a consortium including Legend Capital. History of security vulnerabilities. Supplies accessories/printers to Dell.	Various.
Lishen Power Battery Systems Co. Ltd.	State-owned	CETC is sole shareholder. Supplies batteries to Dell.	State-owned company according to Dow Jones.
Tianma Microelectronics (USA) Inc. .	State-owned	Owned by China defense supplier. Supplies displays to Microsoft	20.81 percent owned by AVIC International Holdings Ltd. and 11.35 percent owned by the State-Owned Assets Supervision and Administration Commission.

50 "U.S. Tech Companies and Their Chinese Partners with Military Ties," *The New York Times*, October 30, 2015, https://www.nytimes.com/interactive/2015/10/30/technology/US-Tech-Firms-and-Their-Chinese-Partnerships.html.

Entity Name	Risk	Details	Source
TPV Technology Ltd.	State-owned	Supplies display/liquid crystal display to Dell and HP.	37.05 percent owned by the State-Owned Assets Supervision and Administration Commission.
Tsinghua Holdings	State-controlled	Asset management group focused on technology and defense sector. Joint ventures and strategic partnerships with Intel, HP, Dell, and IBM.	State-owned company according to Dow Jones.
Shenzhen Laibao Hi-Tech Co. Ltd	State-owned	Supplies display/liquid crystal display to Dell and HP.	20.91 percent owned by the State-Owned Assets Supervision and Administration Commission.
Zhongxing Telecommunications Corporation	National champion	Cyberespionage risk.	U.S. House Permanent Select Committee on Intelligence Investigative Report.

Source: Interos Solutions.

Entities that present the most risk to the supply chain are those that exhibit close ties to Chinese government entities, particularly entities involved in China's military, nuclear, or cyberespionage programs. For example:

- Dell supplier Lishen Power Battery Systems Co. Ltd. is a subsidiary of Tianjin Lishen Battery Joint-Stock Company Limited, an SOE affiliated with CETC, which is a network of former military labs that operates both commercial and military technology businesses. CETC appears to be Lishen's sole shareholder.[51]

- Hengdian Group DMEGC Magnetics Co. Ltd. supplies magnetic materials to Microsoft, and is a subsidiary of Hengdian Group Holdings. The group's website states it is an enterprise approved by the Chinese Academy of Sciences (CAS) and China's Ministry of Science and Technology, and has cooperated with the state-owned China National Nuclear Corporation.[52]

- GoerTek Inc. supplies acoustic components to Microsoft. In addition to state-backed investment from China International Fund Management Co., Ltd., the company has long-term strategic partnerships with the CAS and universities linked to China's cyberespionage programs, such as Tsinghua University, Zhejiang University, and Harbin Institute of Technology.[53] Other customers include Lenovo.[54]

The connections between these firms and entities involved in China's military, nuclear, or cyberespionage programs increase risk associated with federal ICT providers sourcing products or services from these firms. This risk could present itself as a supply chain attack through a compromised product, such as batteries or acoustic components supplied to federal ICT providers. Still other Chinese SOEs supply federal ICT providers with magnets, shielding materials, or cables and power connectors.[55] These products could present risk if they are of inferior quality and fail to operate, but they are unlikely to present significant cybersecurity risk to federal ICT networks. The risk might also stem from more subtle actions, including by federal ICT providers revealing design information, product specifications, or other sensitive information to their suppliers as part of standard business practices. Business information that may be innocuous when passed to a standard business partner becomes less innocuous when passed to individuals or entities associated with a rival government.

A good SCRM program assesses the risks associated with the nature of a particular product in tandem with the risks stemming from the entity that is producing or providing the product. Assessing the supply chain risks associated with liquid crystal displays (LCDs) is one example of this process. Displays are not as critical to an end-product

51 "Shareholder's Info," Lishen, About Lishen, accessed October 29, 2017, http://en.lishen.com.cn/textContent.aspx?cateid=181&bigcateid=171.
52 "History," Hengdian Group, About Us, accessed March 23, 2018, from Internet Archive WayBackMachine, https://web.archive.org/web/20170415230303/http://www.hengdian.com/site/en/en_com_history.htm.
53 "Partners," Goertek, About Us, accessed March 23, 2018, http://www.goertek.com/en/about/hzhb.html.
54 "Goertek Announces Next-Gen VR Reference Design Powered by Snapdragon™ 845," PRNewswire, March 2, 2018, https://www.prnewswire.com/news-releases/goertek-announces-next-gen-vr-reference-design-powered-by-snapdragon-845-300607312.html.
55 "HP Suppliers," Hewlett-Packard; "Our Suppliers," Dell; "Microsoft Top 100 Production Suppliers," Microsoft.

as its microprocessor, but their hardware, firmware, and connections to other ICT products can make them an important component in an ICT supply chain. In 2016, security researchers from Red Balloon Security identified vulnerabilities that allowed hackers to surveil and manipulate users by hacking the embedded firmware of their monitor displays.[56]

Several Chinese companies manufacture the LCDs that are a component of tablets, notebooks, and other computers produced by Microsoft, Dell, HP, and other federal ICT providers, and several of these companies have ties to the Chinese government or military. For example:

- Tianma Microelectronics supplies LCDs to Microsoft. The company's primary shareholders include AVIC International Holdings Ltd., the State-Owned Assets Supervision and Administration Commission (which manages the central government's SOEs), and the City of Wuhan. AVIC is an SOE that was formed in 2008 after the consolidation of China Aviation Industry Corporation I (AVIC I) and China Aviation Industry Corporation II (AVIC II).[57] AVIC is also one of China's largest defense suppliers, and makes aircraft for civilian and military uses, including bombers and fighter jets.

- Dell and HP both source LCDs from the state-owned TPV Technology Ltd. and Shenzhen Laibao Hi-Tech Co. Ltd. TPV Technology Ltd. is a China-based company that also does business as Top Victory Electronics Company and TPV-INVENTA Technology Co., Ltd. The company is controlled by state asset groups such as the State-Owned Assets Supervision and Administration Commission and China Greatwall Technology Group Co., Ltd. The State-Owned Assets Supervision and Administration Commission also controls 20 percent of Shenzhen Laibao Hi-Tech Co. Ltd. Dell also sources LCDs from six sites controlled by BOE Global, a company whose largest shareholder is the Beijing state-owned Capital Management Center.[58]

SUPPLY CHAIN RISK CASE STUDY: CORPORATE INTELLIGENCE-SHARING AGREEMENTS

An analysis of the business relationships of several top federal government ICT providers reveals corporate alliances and partnerships with SOEs in China as well as government-connected firms in Israel and Russia. Business relationships can affect multiple tiers within a single supply chain. While such networks of corporate alliance and partnership are common in the commercial sphere, they present security risks to federal ICT systems by potentially allowing nefarious actors access to technical information that could be used to infiltrate federal ICT systems. The information sharing inherent in commercial alliances can enable more efficient product integration and development. Commercial partnerships that share program application data, configuration information, or even deployment policies, however, may inadvertently grant malicious actors information they need to infiltrate federal ICT systems. Without a comprehensive SCRM program to investigate these partnerships, the connections and relationships may never be known, and the risk may remain undiscovered.

Intel and IBM: (In)Security Partnerships

Concerns associated with component production and manufacturing in China represent one facet of the supply chain risk facing the federal government's ICT system. As Chinese companies move up the value chain, the prospect of China-supplied software becomes ever more important to risk analysis. While an analysis of source code is generally not possible from unclassified sources, supply chain risks can be assessed on the basis of published business partnership announcements, including the establishment of corporate alliances.

Intel's Security Innovation Alliance allows partner companies to exchange threat intelligence and develop technology integrations with the McAfee Data Exchange Layer. The alliance produces integrated security solutions, by allowing technology partners to connect their products in a more efficient manner. The alliance includes companies (such as Huawei) with connections to the governments and security organizations of countries on

56 Lorenzo Franceschi-Bicchierai, "Hackers Could Break into Your Monitor to Spy on You and Manipulate Your Pixels," *Motherboard*, August 6, 2016, https://motherboard.vice.com/en_us/article/jpgdzb/hackers-could-break-into-your-monitor-to-spy-on-you-and-manipulate-your-pixels.
57 "Overview," AVIC, About Us, accessed October 29, 2017, http://www.avic.com/en/aboutus/overview/index.shtml.
58 Lexis Nexis, Dun and Bradstreet, Dow Jones, Hoovers Data Repository. Factiva Database, Dow Jones and Reuters, New York.

the intelligence community's sensitive countries list.[59] As part of the alliance, Huawei provides a Cybersecurity Intelligence System that collects network traffic information in order to detect attacks and provide investigation and evidence collection capabilities. Huawei Cybersecurity Intelligence System works with McAfee ePolicy Orchestrator and McAfee Active Response. Partner products are subject to engineering testing prior to integration, but the risk in these partnerships stems from the possibility that information, source code, or other details shared as part of the product integration process could also be used to identify and exploit vulnerabilities in a product.

In a 2012 report, Gartner noted that the technical challenges of technology integration and corporate collaboration present increasing risk to ICT supply chains: "Enterprises are opening up their internal IT networks and systems to collaborate and share information with customers, partners and suppliers. As a result, all of these become targets for IT supply chain compromise."[60] Intel is not alone in participating in these sorts of alliances. In 2000, IBM announced a collaborative agreement with Huawei, including an R&D effort.[61]

VMware Partnerships with Chinese SOEs and Kaspersky

VMware, a subsidiary of Dell, has entered into corporate partnerships with Chinese SOEs that could present national security vulnerabilities to U.S. federal ICT systems. VMware provides cloud computing and software virtualization services to the U.S. government and the private sector. Following Dell's acquisition of VMware's parent company, EMC, in September 2016, Dell controls approximately 82.8 percent of VMware's outstanding common stock.[62]

In April 2016, VMware set up its first China joint venture with Sugon, a Tianjin-based company that specializes in high-performance computers, servers, storage products, and software systems. Sugon's full English name is Dawning Information Industry. It was founded as Dawning Yunjisuan Technology Co. Ltd. in 1996 with backing from the CAS. Currently the Chinese government is the largest shareholder of Sugon, with the CAS retaining a 23 percent stake.[63] The VMware-Sugon joint venture is called VMsoft and provides cloud computing and virtualization software and services. VMware holds a 49 percent stake in VMsoft, while Sugon holds a 51 percent stake.[64]

VMware also has product relationships with Kaspersky Lab,[65] the Russia-based cybersecurity and antivirus software company recently named in the DHS's divestment directive.[66] Kaspersky is a Russian-owned cybersecurity provider whose founder and CEO used to work for the KGB, the security service of the former Soviet Union.[67] A recent reported shift in the leadership of Kaspersky Labs has seen people with close ties to Russian military and intelligence services filling more executive positions. Speculation exists that these executives actually participate

59 Warwick Ashford, "Check Point, Huawei Join Intel Security Innovation Alliance," *Computer Weekly*, November 3, 2016, http://www.computerweekly.com/news/450402310/Check-Point-Huawei-join-Intel-Security-Innovation-Alliance; "Huawei Joins Intel Security Innovation Alliance to Defend Customers against Security Threats," Huawei, News, November 4, 2016, http://www.huawei.com/en/news/2016/11/Huawei-Joins-Intel-Security-Innovation-Alliance; "McAfee Security Innovation Alliance Partner Directory," McAfee, Business Home, Partners, McAfee Security Innovation Alliance, accessed October 29, 2017, https://www.mcafee.com/us/partners/partnerlisting.aspx.

60 "Maverick*Research: Living in a World without Trust: When IT's Supply Chain Integrity and Online Infrastructure Get Pwned," Gartner, October 5, 2012, http://www.energycollection.us/Energy-Security/Living-World-Without-Trust-Filed.pdf.

61 IBM, "IBM and Huawei Announce Networking Technology Collaboration," news release, September 25, 2000, https://www-03.ibm.com/press/us/en/pressrelease/1541.wss.

62 VMware, Inc., "10-K Annual Report 2016," retrieved October 25, 2017, from SEC EDGAR database, https://www.sec.gov/Archives/edgar/data/1124610/000112461017000009/vmw-1231201610xk.htm.

63 Tom Wilkie, "Chinese Government Kicks Commercial Companies Overseas," *Scientific Computing World*, August 25, 2015, https://www.scientific-computing.com/feature/chinese-government-kicks-commercial-companies-overseas.

64 Jane Ho, "VMware Sets up First China Joint Venture with High-Performance Computer Maker Sugon," *Forbes*, May 24, 2016, https://www.forbes.com/sites/janeho/2016/05/24/VMware-sets-up-first-china-joint-venture-with-high-performance-computer-maker-sugon/#257d64db20af.

65 "Kaspersky Agentless Virtualization Security," Kaspersky, Products, accessed October 30, 2017, https://usa.kaspersky.com/small-to-medium-business-security/virtualization-agentless; Department of Homeland Security, "DHS Statement on the Issuance of Binding Operational Directive 17-01," press release, September 13, 2017, https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01; "Kaspersky Security for Virtualization 3.0 Agentless Service Pack 1 (2134021)," VMware, last updated October 16, 2015, https://kb.vmware.com/s/article/2134021.

66 On September 13, 2017, the DHS issued a directive ordering federal departments and agencies to identify, discontinue to use, and ultimately remove the Kaspersky products from federal information systems. This directive was issued amid concerns that the Russian government and Russian intelligence agencies may use Kaspersky products to compromise federal information systems.

67 Pamela Engel, "Why One of the World's Leading Cyber-espionage Firms Won't Touch Russia," *Business Insider*, March 19, 2015, http://www.businessinsider.com/kaspersky-and-russian-spies-2015-3.

in investigations on behalf of the Russian government and may share Kaspersky customers' data with the government.[68] Reports by *BloombergBusinessweek* from July 2017 cited internal Kaspersky emails alleging that Kaspersky personnel have accompanied Russian intelligence and police on raids and arrests.[69] A report from *The Wall Street Journal* in October 2017 shed additional light on an incident in 2015, in which hackers working for the Russian government used Kaspersky's antivirus software running on an NSA contractor's personal computer to steal details about how the United States penetrates foreign computer networks and defends against cyberattacks.[70] The U.S. government has been progressively blocking agencies from using Kaspersky. The National Defense Authorization Act for Fiscal Year 2018, signed into law in December 2017, included a ban on using "hardware, software, or services developed or provided, in whole or in part" by Kaspersky Lab, its successors, or affiliated entities.[71]

These types of business relationships can introduce risk through multiple relationships at different tiers within a single supply chain. Kaspersky's products integrate with virtual machine platforms such as Microsoft Hyper-V, Citrix XenServer, and Kernel-based Virtual Machine.[72] Kaspersky is a "VMware Integrated Partner Solutions for Networking and Security" provider, as well as one of the six partners VMware recommends for antivirus and protection solutions.[73] VMware also has a relationship with vArmour Networks, Inc., a virtual data center and cloud security company,[74] and vArmour has a partnership with Nutanix, which is itself a technology partner of Kaspersky.[75] Kaspersky antivirus products are integrated into routers, chips, and software products produced by Cisco, Juniper, D-Link, Broadcom, Amazon, and Microsoft.[76]

68 Carol Matlack, Michael Riley, and Jordan Robertson, "The Company Securing Your Internet Has Close Ties to Russian Spies," *BloombergBusinessweek*, March 20, 2015, https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies.

69 Jordan Robertson and Michael Riley, "Kaspersky Lab Has Been Working with Russian Intelligence," *BloombergBusinessweek*, July 11, 2017, https://www.bloomberg.com/news/articles/2017-07-11/kaspersky-lab-has-been-working-with-russian-intelligence.

70 Gordon Lubold and Shane Harris, "Russian Hackers Stole NSA Data on U.S. Cyber Defense," *The Wall Street Journal*, October 5, 2017, https://www.wsj.com/articles/russian-hackers-stole-nsa-data-on-u-s-cyber-defense-1507222108.

71 National Defense Authorization Act for Fiscal Year 2018.

72 "Kaspersky Security for Virtualization," Kaspersky Lab, accessed October 30, 2017, http://media.kaspersky.com/en/business-security/Kaspersky%20Security%20for%20Virtualization%20Datasheet.pdf.

73 "VMware Integrated Partner Solutions for Networking and Security," VMware, accessed October 30, 2017, https://www.VMware.com/content/dam/digitalmarketing/VMware/en/pdf/products/vcns/VMware-integrated-partner-solutions-networking-security.pdf; "Antivirus Best Practices for VMware Horizon View 5.x," VMware, accessed October 30, 2017, https://www.VMware.com/content/dam/digitalmarketing/VMware/en/pdf/techpaper/VMware-View-AntiVirusPractices-TN-EN.pdf.

74 vArmour, "vArmour Distributed Security System Achieves VMware's Highest Level of Product Endorsement–VMware Ready," press release, September 16, 2015. https://www.varmour.com/past-press/94-varmour-distributed-security-system-achieves-VMware-s-highest-level-of-product-endorsement-VMware-ready.

75 Keith Stewart, "It's Official: vArmour and Nutanix Team up to Deliver Simple, Secure Data Centers," vArmour blog, July 8, 2015, https://www.varmour.com/resources/blog/entry/its-official-varmour-and-nutanix-team-up-to-deliver-simple-secure-data-centers; "vArmour," Nutanix, Technology Alliances, accessed October 30, 2017, https://www.nutanix.com/partners/technology-alliance-program/varmour/; "vArmour and Nutanix Partner to Simplify and Secure Hyper-Converged, Distributed Infrastructure," *Martekwired*, July 8, 2015, https://finance.yahoo.com/news/varmour-nutanix-partner-simplify-secure-120000717.html; "Recognition," Kaspersky, Solutions, Enterprise Security, Cloud Security, accessed October 30, 2017, https://usa.kaspersky.com/enterprise-security/virtualization.

76 Adam Mazmanian, "Kaspersky Axed from Governmentwide Contracts," *FCW*, July 12, 2017, https://fcw.com/articles/2017/07/12/kaspersky-gsa-nasa-intel.aspx.

Chapter 4: China's Political and Economic Agenda Is Behind the Supply Chain Security Dilemma

Understanding that Chinese national political and economic policies encourage indigenous ICT manufacturing and development helps explain the risks to the U.S. ICT supply chain. The PRC government justifies these policies in terms of ensuring China's own national security, but China's policies related to prioritizing indigenous production, extracting concessions from multinationals, using Chinese companies as state tools, and targeting U.S. federal networks and the networks of federal contractors have heightened risks to the U.S. ICT supply chain.

PRIORITIZING INDIGENOUS ICT PRODUCTION

The Chinese government has expended significant political and economic capital in its effort to expand and indigenize its ICT production capabilities. In the 1980s, China began to rival Japan and South Korea as a producer of low-tech IT components. China's production capacity expanded throughout the 1990s, and it began to move up the value chain, producing ever more complex electronic equipment. By the late 1990s, the Chinese domestic market itself became a factor in the evolving equation. The rising incomes of China's new middle class meant that the country was now an important consumer market for the very products it had once been known for producing and exporting. Multinational tech companies shifted production and supply centers to China, launched Chinese subsidiaries, and invested in Chinese manufacturing and R&D centers to meet demand from China's rapidly growing domestic market. These deals occurred in tandem with PRC outreach to foreign multinationals, as the country encouraged foreign investment that could bring new products, technologies, and, most important, jobs to China. **Table 3** is an overview of key PRC policies enacted during this period.

Table 3
Foundational PRC Policies for Indigenous ICT Development

Date	Title	Description
1986	National High Technology Research and Development Program (863 Program)	The 863 Program funds high-technology development in strategic sectors, including IT, biology, aeronautics, automation, energy, materials, and oceanography. Government institutes, university research labs, and SOE R&D departments participate in 863 initiatives. The Chinese Academy of Sciences is the largest recipient of 863 money. In 2014, the program provided more than $5 billion for China's microchip industry, developing software to compete with Microsoft's Windows and Google Inc.'s Android, and advancing China's server manufacturing capacity. Inspur Chairman Sun Pishu is a member of China's legislature and a member of the 863 Program's expert committee. In 2014, he proposed measures to review critical technology purchases and accelerate domestic innovation efforts.
2006	National Medium- and Long-Term Plan for Science and Technology Development Plan (2006–2020)	The goal is for China to be a major center of indigenous innovation by 2020 and a global innovation leader by 2050. This plan: • Seeks to sharply reduce the country's dependence on foreign technology • Increases gross expenditures for R&D, especially for space programs, aerospace development and manufacturing, renewable energy, computer science, and life sciences • Calls for regulations in the country's government procurement law to "encourage and protect indigenous innovation," requiring a first-buy policy for major domestically made high-tech equipment and products that possess proprietary intellectual property rights, providing policy support to enterprises in procuring domestic high-tech equipment, and developing "relevant technology standards" through government procurement

Source: James McGregor, Dow Jones.[77]

77 James McGregor, *China's Drive for "Indigenous Innovation": A Web of Industrial Policies* (Washington, DC: U.S. Chamber of Commerce, Global Regulatory Cooperation Project, 2010), https://www.uschamber.com/sites/default/files/documents/files/100728chinareport_0_0.pdf; Dow Jones, "NSA Concerns Give Chinese Server Maker Inspur a Boost," *The Australian*, July 30, 2014, http://www.theaustralian.com.au/business/latest/nsa-concerns-give-chinese-server-maker-inspur-a-boost/news-story/b80feaa88eb98909ad47ea1bc11ae948.

In February 2017, the PRC State Council published a press release highlighting a recent IHS Markit report indicating China has moved from being a low-cost supplier to being the center of the global supply chain.[78] As Chinese firms move up the value chain, the Chinese government has shifted the focus of its development policies. Where once the PRC government offered tax incentives and other perks to encourage foreign direct investment (FDI), the Chinese domestic market now represents a significant draw. China is less likely to offer incentives to foreign companies to do business in China and more likely to demand concessions from them in exchange for the privilege, thereby creating even more opportunities for risk insertion into the global COTS ICT supply chain.

RAISING SECURITY CONCERNS

Since 2013, the Chinese government has put pressure on U.S. ICT companies to surrender source code, store data on servers based in China, invest in Chinese companies, and permit the PRC government to conduct security audits on ICT products. In the wake of Edward Snowden's 2013 allegations that the U.S. government used some of the country's technology firms to spy on foreign governments, Chinese officials began investigating Microsoft, Apple, and other U.S. technology companies.[79] Official media called for a "de-Cisco campaign" or a boycott of Cisco products.[80] In June 2013, the Chinese state-backed *China Economic Weekly* ran a cover story calling eight U.S. companies (Apple, Cisco, Google, IBM, Intel, Microsoft, Oracle, and Qualcomm) "guardian warriors" that had "seamlessly penetrated" Chinese society.[81]

Several elements of subliminal messaging are at work here. In a move directed primarily at U.S. observers and China's educated and globalized elite, the cover of the issue that contained this article reused a U.S. World War II poster originally released to warn against German espionage.[82] **Exhibit 3** compares the two images. The image on the left is a copy of the original poster released by the U.S. Office of Emergency Management in 1942. The image on the right is the cover of *China Economic Weekly* published in June 2013, modified by the addition of the NSA insignia on the soldier's helmet.

Exhibit 3
U.S. Espionage Drives China's Nationalist IT Policy

Sources: U.S. Office of Emergency Management (1942) and *China Economic Weekly* (2013).

78 "China Becomes Center of Global Supply Chain," State Council of the People's Republic of China, February 10, 2017, http://english.gov.cn/news/top_news/2017/02/10/content_281475564088064.htm.
79 Eva Dou, "NSA Concerns Give Chinese Server Maker a Boost," *The Wall Street Journal*, July 29, 2014, https://www.wsj.com/articles/nsa-concerns-give-chinese-server-maker-inspur-a-boost-1406653858.
80 Daniel H. Rosen and Beibei Bao, "Eight Guardian Warriors: PRISM and Its Implications for US Businesses in China," Rhodium Group, July 18, 2013, http://rhg.com/notes/eight-guardian-warriors-prism-and-its-implications-for-us-businesses-in-china-2.
81 Bai Zhaoyang 白朝阳, "Meiguo 'Bada Jingang' Shentou Zhongguo Da Qi Di" 美国"八大金刚"渗透中国大起底 [United States' "Eight Guardian Warriors" Seamlessly Penetrate China], *China Economic Weekly* 中国经济周刊, June 24, 2013, http://paper.people.com.cn/zgjjzk/html/2013-06/24/content_1259857.htm.
82 United States Office of Emergency Management, "He's Watching You" (1942), accessed from New Hampshire State Library, Unifying a Nation, https://www.nh.gov/nhsl/ww2/ww57.html.

More relevant to China's domestic audience, the labeling of the eight U.S. tech firms as "guardian warriors" recalls the Eight-Nation Alliance that intervened militarily in China between 1899 and 1901 to suppress the Boxer Rebellion. Views on the rebellion are diverse, but in general the episode marked the flagging legitimacy of the Qing dynasty and the growing strength of anti-foreign, anti-colonialist forces in Chinese politics. Current PRC rhetoric frequently couches the Boxer Rebellion in anti-imperialist, patriotic-nationalist terms, and the Eight-Nation Alliance as a group that facilitated the collapse of the last Chinese dynasty and foreign oppression. The eight guardian warriors, then, represent not only a pernicious threat to China's unity and independence but also a call for increased self-reliance in order to resist foreign influence. The *China Economic Weekly* article argues that while President Barack Obama made it illegal for U.S. agencies to purchase Chinese IT equipment without a federal cybersecurity investigation, no law requiring the investigation of U.S. companies yet existed in China.

In 2014, more allegations about NSA espionage efforts directed at China were reported by the German weekly *Der Spiegel* and the *New York Times*.[83] The reports alleged that in early 2009 the NSA began targeting Huawei, as well as Chinese ministries, banks, and then-president Hu Jintao. The Chinese government began to move against U.S. ICT companies soon after, launching antitrust investigations of Qualcomm and Microsoft, issuing a ban on Windows 8 on government computers, and raising concerns about the Apple iPhone's security. In response to this pressure, Apple has promised to build an R&D center in China.[84]

EXTRACTING CONCESSIONS FROM MULTINATIONALS

The FDI Regulatory Restrictiveness Index of the Organisation for Economic Co-operation and Development (OECD) measures statutory restrictions on FDI in 62 countries, including all OECD and G20 countries, and covers 22 sectors.[85] The index gauges the restrictiveness of a country's FDI rules by looking at the four main types of restrictions: (1) foreign equity limitations, (2) screening or approval mechanisms, (3) restrictions on the employment of foreigners as key personnel, and (4) operational restrictions such as restrictions on branching, capital repatriation, or land ownership. According to OECD data, China is the most restrictive of the G20 countries.[86]

In 2014 and 2015, the Chinese government ramped up implementation of laws and policies that raise market access concerns among ICT manufacturers and suppliers in the United States by threatening to decrease competition, favor Chinese firms over foreign firms, or extract concessions from multinational firms seeking to do business in China. Many of these laws and policies are discussed in depth in publications by the U.S. Chamber of Commerce, the Congressional Research Service, and the U.S.-China Economic and Security Review Commission.[87] **Table 4** offers a brief overview.

83 "NSA Spied on Chinese Government and Networking Firm," *Der Spiegel*, March 22, 2014, http://www.spiegel.de/international/world/nsa-spied-on-chinese-government-and-networking-firm-huawei-a-960199.html; David E. Sanger and Nicole Perlroth, "N.S.A. Breached Chinese Servers Seen as Security Threat," *The New York Times*, March 22, 2014, https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html.

84 David Barboza, "How China Built 'iPhone City' with Billions in Perks for Apple's Partner," *The New York Times*, December 29, 2016, https://www.nytimes.com/2016/12/29/technology/apple-iphone-china-foxconn.html.

85 "FDI Regulatory Restrictiveness Index," Organisation for Economic Co-operation and Development, March 27, 2017, http://www.oecd.org/investment/fdiindex.htm.

86 The Group of Twenty (G20) is an international forum dedicated to international cooperation on financial and economic issues. Members of the G20 include many of the world's wealthiest nations, and collectively account for more than four-fifths of the world's gross domestic product, three-quarters of global trade, and almost two-thirds of the world's population.

87 James McGregor, *China's Drive for "Indigenous Innovation"*; Wayne M. Morrison, "China-U.S. Trade Issues," Congressional Research Service, February 9, 2017, 35; OECD, OECD Science, Technology and Innovation Outlook 2016; Nargiza Salidjanova et al., "Economics and Trade Bulletin," U.S.-China Economic and Security Review Commission, August 7, 2017, https://www.uscc.gov/sites/default/files/Research/August%202017%20Trade%20Bulletin.pdf; "Economics and Trade Bulletin," U.S.-China Economic and Security Review Commission, June 2, 2017, https://www.uscc.gov/sites/default/files/trade_bulletins/June%202017%20Trade%20Bulletin.pdf.

Table 4
Chinese Laws and Policies Related to ICT and National Security

Date Issued	Title	Description
May 2015	Notice of the State Council on Issuing "Made in China 2025"	Lays out a comprehensive plan to upgrade the Chinese manufacturing sector through the use of intelligent ICT (smart manufacturing). Sets nine priority tasks over 10 sectors, with five definitive projects, including new IT, robotics, aerospace, ocean engineering, and high-end rail transportation. Calls for strengthened security reviews for investment, mergers and acquisitions, and procurement in manufacturing sectors that are related to national economy and national security.
July 2015	National Security Law	Promotes domestic and indigenous innovation in key sectors. Enables the government to conduct "national security reviews" of "foreign commercial investment, special items and technologies, Internet information technology products and services, projects involving national security matters, as well as other major matters and activities, that impact or might impact national security."
July 2015	Guiding Opinions of the State Council on Actively Advancing "Internet+" Action	Aims to drive economic growth in China through the integration of internet technologies with manufacturing and business. Prioritizes upgrading and strengthening the security of the internet infrastructure, expanding access to the internet and related technologies, making social services more convenient and effective, and increasing both the quality and effectiveness of economic development.
January 2016	Counter-Terrorism Law	Requires telecommunications operators and internet service providers to provide technical interfaces, decryption, and other technical support assistance to public and state security organizations that are conducting activities to prevent or investigate terrorism.
July 2016	13th Five-Year Plan for Science and Technology Innovation	Aims to strengthen China's science and technology competitiveness and international influence and develop breakthroughs in core and critical technology areas in order to support economic restructuring and industrial upgrading.
November 2016	Cybersecurity Law	Restricts select data transfers out of China. Requires firms that fall under the critical information infrastructure to store their data inside China. Firms have until 2018 to comply with some data storage requirements. Requires firms that interact with the critical information infrastructure or that provide services that may affect national security to be subject to a security review by Chinese authorities. This review may be used to ensure that these services are "secure and controllable," a term used in other Chinese digital regulations, which compels foreign firms to hand over important intellectual property assets such as source code to Chinese authorities for inspection.
November 2017	Standardization Law of People's Republic of China	Revises China's 1989 Standardization Law in ways that may advantage Chinese companies over U.S. and other non-Chinese companies. During its investigation into China's practices related to intellectual property and technology transfer, the Office of the United States Trade Representative determined the standards may require U.S. companies to make product or service-related disclosures that increase costs and/or risks.

Sources: McGregor, Morrison, OECD, Salidjanova et al., U.S.-China Economic and Security Review Commission, U.S. Chamber of Commerce, Office of the U.S. Trade Representative.

The U.S. Chamber of Commerce produced reports in 2016 and 2017 detailing trade policies between the United States and China, particularly as they relate to ICT products.[88] The shift in tone over the course of a year is revealing.

88 U.S. Chamber of Commerce, *Preventing Deglobalization: An Economic and Security Argument for Free Trade and Investment in ICT* (Washington, DC: U.S. Chamber of Commerce, 2016), https://www.uschamber.com/sites/default/files/documents/files/preventing_deglobalization_1.pdf; U.S. Chamber of Commerce, *Made in China 2025: Global Ambitions Built on Local Protections* (Washington, DC: U.S. Chamber of Commerce, 2017), https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf.

The 2016 paper is cautiously optimistic that increasing trends to "deglobalize" trade could be reversed. The 2017 paper paints a darker view, seemingly more certain that China's course is increasingly set toward balkanization and creating disadvantages for foreign companies in support of domestic competitors and indigenous innovation.

These new regulations present a serious dilemma for U.S. multinationals and a threat to U.S. national security. If U.S. multinationals fail to adhere to Chinese government regulations, they may face restricted market access in China, which could decrease their revenues and global competitiveness. But if U.S. companies—which are the primary providers of ICT to the U.S. federal government—surrender source code, proprietary business information, and security information to the Chinese government, they open themselves and federal ICT networks to Chinese cyberespionage efforts.

This threat is not theoretical. Chinese government pressure on companies to submit source code for review may occur in support of, or in tandem with, other efforts to identify vulnerabilities in U.S. ICT products. The China Information Technology Evaluation Center (CNITSEC), which conducts the security reviews of foreign companies, is run by China's Ministry of State Security. But Recorded Future, a U.S.-Swedish internet technology company focusing on cyber intelligence, has linked CNITSEC to APT3, a China-based cyberespionage unit that has hacked federal agencies and companies in the United States and Hong Kong.[89]

Microsoft has allowed the Chinese government to access its source code since 2003, when it signed an agreement with CNITSEC allowing China to participate in its Government Security Program, which grants access to the source code and technical information of several versions of Windows software.[90] In January 2010, 34 U.S. companies, including Google, Adobe, Yahoo, and Northrop Grumman, were hit by attacks from China facilitated by a previously unknown vulnerability in Microsoft's Internet Explorer. In March 2010, researchers at McAfee claimed the January attacks targeted the companies' source-code management systems in an effort to extract proprietary source code.[91]

Reports from *The Guardian* indicate that the Microsoft source code used in the attacks was obtained from Chinese IT security companies. *The Guardian*'s reporting indicates CNITSEC and its partner, Topsec, may have passed Microsoft source code to the Chinese government units that carried out the hacking.[92] Topsec's connection to the Chinese government includes work related to China's space program, its national firewall, and other high-profile state projects, such as the 2008 Olympic Games, the 2010 World Expo, and the 2010 Guangzhou Asian Games.[93]

In October 2015, IBM became the first major U.S. tech company to allow officials from China's Ministry of Industry and Information Technology to examine its proprietary source code.[94] In September 2016, Microsoft announced the opening of its new Microsoft Transparency Center in Beijing, China, which will allow government officials to analyze and test products.[95] Additional Transparency Centers are located in Belgium, Brazil, Singapore, and the United States.[96]

89 Insikt Group, "Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3," *Recorded Future* (blog), May 17, 2017, https://www.recordedfuture.com/chinese-mss-behind-apt3/; Mark Rockwell, "Feds Targeted in Clandestine Wolf Phishing Campaign," *FCW*, July 13, 2015, https://fcw.com/articles/2015/07/13/fed-phishing.aspx.

90 "Microsoft and China Announce Government Security Program Agreement," Microsoft, February 28, 2003, https://news.microsoft.com/2003/02/28/microsoft-and-china-announce-government-security-program-agreement/.

91 Kim Zetter, "Google Hackers Had Ability to Alter Source Code," *Wired*, March 3, 2010, https://www.wired.com/2010/03/source-code-hacks/.

92 Pascal-Emmanuel Gobry, "China Used Microsoft Source Code to Hack Google—And You?" *Business Insider*, December 7, 2010, http://www.businessinsider.com/wikileaks-china--microsoft-source-hack-google-2010-12.

93 "Introduction to TOPSEC," Topsec, http://www.topsec.com.cn/english/about_us.html.

94 Eva Dou, "IBM Allows Chinese Government to Review Source Code," *The Wall Street Journal*, October 16, 2015, https://www.wsj.com/articles/ibm-allows-chinese-government-to-review-source-code-1444989039.

95 Scott Charney, "New Beijing Transparency Center Announced," Microsoft, September 19, 2016, https://blogs.microsoft.com/on-the-issues/2016/09/19/new-beijing-transparency-center-announced/.

96 "Government Security Program," Microsoft, June 2017, http://az370354.vo.msecnd.net/enterprise/GSP%20External%20Content%20Overview%20-%20Trust%20Center%20Version.pdf.

USING CHINESE COMPANIES TO FURTHER STATE GOALS

China is not a U.S. ally and is not likely to become one anytime soon. Moreover, the Chinese government and actors associated with it have repeatedly engaged in well-documented instances of theft and misuse of IP, as well as state-directed economic espionage. Chinese government policies summarized in **Table 4** are aimed at, among other goals, the creation and support of Chinese national champions—companies that further the government's strategic aims in return for government support.

Government support can take many forms, but it often includes preferential financing rates, preference in government contract bidding, and sometimes oligarchy or monopoly status in protected industries.[97] In the case of Chinese national champions, the support also appears to include officially sanctioned or officially conducted corporate espionage designed to improve the competitiveness of Chinese firms while potentially advancing other government interests.[98] Huawei, Zhongxing Telecommunications Corporation (ZTE), and Lenovo are three Chinese ICT companies that exhibit some of these characteristics.

Huawei is a Chinese multinational networking and telecommunications equipment company headquartered in Shenzhen.[99] Ren Zhengfei, a former officer in the People's Liberation Army (PLA) and a military technology researcher, founded Huawei in 1987 and continues to operate it.[100] Although Huawei is registered as a private company, a report by the U.S. House of Representatives Permanent Select Committee on Intelligence says Huawei:[101]

> *operates in what Beijing explicitly refers to as one of seven "strategic sectors." Strategic sectors are those considered as core to the national and security interests of the state. In these sectors, the CCP [Chinese Communist Party] ensures that "national champions" dominate through a combination of market protectionism, cheap loans, tax and subsidy programs, and diplomatic support in the case of offshore markets. Indeed, it is not possible to thrive in one of China's strategic sectors without regime largesse and approval.*

Huawei claims to be employee owned, but the company, unlike many Chinese corporations, has chosen not to sell shares in Hong Kong or the United States, which would require it to make financial disclosures.[102]

As early as 2000, hackers who appeared to be located in China infiltrated and exploited the networks of Nortel Networks Ltd., a foreign competitor of Huawei. Nortel was a multinational telecommunications and data networking equipment manufacturer headquartered in Canada. Nortel discovered the hacking in 2004 and determined that the hackers had obtained the passwords of seven top officials, including a previous CEO. Using China-based internet addresses, the hackers downloaded technical papers, R&D reports, and business plans, and monitored the employee email system.[103] The Nortel employee who conducted the internal investigation alleged that the hackers were based in Shanghai. Outside expert analysis determined that the rootkits installed on Nortel's systems were the work of professionals.[104]

---

97 Antonio Graceffo, "China's National Champions: State Support Makes Chinese Companies Dominant," *Foreign Policy Journal*, May 15, 2017, https://www.foreignpolicyjournal.com/2017/05/15/chinas-national-champions-state-support-makes-chinese-companies-dominant/.

98 Shane Harris, "Exclusive: Inside the FBI's Fight against Chinese Cyber-Espionage," Foreign Policy, May 27, 2014, http://foreignpolicy.com/2014/05/27/exclusive-inside-the-fbis-fight-against-chinese-cyber-espionage/; Cyber Espionage and the Theft of U.S. Intellectual Property and Technology, *Testimony Before the House of Representatives Committee on Energy and Commerce Subcommittee on Oversight and Investigations* (July 9, 2013) (statement by Larry M. Wortzel), http://docs.house.gov/meetings/IF/IF02/20130709/101104/HHRG-113-IF02-Wstate-WortzelL-20130709-U1.pdf.

99 "Corporate Information," Huawei, accessed September 21, 2017, http://www.huawei.com/en/about-huawei.

100 Michael S. Schmidt, Keith Bradsher, and Christine Hauser, "U.S. Panel Cites Risks in Chinese Equipment," *The New York Times*, October 8, 2012, http://www.nytimes.com/2012/10/09/us/us-panel-calls-huawei-and-zte-national-security-threat.html.

101 Permanent Select Comm. on Intelligence, Investigative *Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE, a Report by Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger of the Permanent Select Committee on Intelligence*, U.S. House of Representatives, 112th Cong. (October 8, 2012), https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.

102 Schmidt, Bradsher, and Hauser, "U.S. Panel Cites Risks in Chinese Equipment."

103 Siobhan Gorman, "Chinese Hackers Suspected in Long-Term Nortel Breach," *The Wall Street Journal*, February 14, 2012, https://www.wsj.com/articles/SB10001424052970203363504577187502201577054.

104 Jameson Berkow, "Nortel Hacked to Pieces," *Financial Post*, February 25, 2012, http://business.financialpost.com/technology/nortel-hacked-to-pieces.

Nortel changed the compromised passwords, but six months later the hackers appeared to retain some access to the company's systems. Every month or so, a few computers on Nortel's network would send small bursts of data to one of the internet addresses in Shanghai involved in the password-hacking episodes. Subsequent investigations revealed that the hackers had installed spyware on Nortel's computers, could control some computers remotely, and had set up an encrypted communication channel to an internet address near Beijing. Nortel filed for bankruptcy in 2009. The hacking incident was not fully disclosed when the company began selling off assets, and reports from former Nortel employees indicate that firms such as Avaya, which acquired Nortel assets following the bankruptcy, may have inadvertently purchased compromised Nortel IT equipment, leaving Avaya's systems vulnerable to infiltration by the same hackers who targeted Nortel.[105] Unconfirmed reports suggest that the hackers who targeted Nortel (as well as Motorola and Cisco during the same period) were working on behalf of Huawei, which had surpassed its U.S. competitor, Cisco, in several core markets.[106]

Huawei has been the subject of numerous investigations and congressional hearings regarding the company's alleged ties to the Chinese Communist Party and the PLA.[107] In February 2011, the Committee on Foreign Investment in the United States issued a recommendation that Huawei voluntarily divest the assets it received in a 2010 deal with 3Leaf, a U.S. company that developed advanced computer technologies. In response, Huawei published an open letter to the U.S. government denying the existence of security issues in the company or its equipment and requesting a full investigation into its corporate operations.[108] The House Permanent Select Committee on Intelligence initiated an investigation into Huawei and ZTE in November 2011 and produced a report in October 2012. The following were among the report's recommendations:

- *U.S. government systems, particularly sensitive systems, should not include Huawei or ZTE equipment, including component parts. Similarly, government contractors—particularly those working on contracts for sensitive U.S. programs—should exclude ZTE or Huawei equipment from their systems.*
- *Private sector entities in the United States are strongly encouraged to consider the long-term security risks associated with doing business with either ZTE or Huawei for equipment or services. U.S. network providers and systems developers are strongly encouraged to seek other vendors for their projects. Based on available classified and unclassified information, Huawei and ZTE cannot be trusted to be free of foreign state influence, and thus pose a security threat to the United States and to our systems.*[109]

Congressional concern with Huawei and ZTE has continued. In January 2018, U.S. Representative Mike Conaway (R-TX) introduced the Defending U.S. Government Communications Act, which would prohibit the U.S. government from purchasing and using "telecommunications equipment and/or services" from Huawei and ZTE.[110]

Huawei and ZTE are not the only Chinese companies to be accused of such activity. The Chinese computer and server manufacturer Lenovo is a similar case. Lenovo originally formed in 1984 as the New Technology Development Company, a component of the state-run Chinese Academy of Sciences Institute of Computing Technology.[111] The founder of Lenovo was educated at the Xi'an Military Communications Engineering Institution of the PLA, now Xidian University. The university has close connections with the PLA and is considered to be a link between China's civilian and military research on cybersecurity.[112] Additionally, Lenovo's CEO, who succeeded its

105 Tom Warren, "Hackers Roamed Nortel's Network for Years without Detection," *The Verge*, February 14, 2012, https://www.theverge.com/2012/2/14/2797047/nortel-undetected-hacking-breach.

106 Mark Anderson, "The Sony Hack and Nortel's Demise: Piracy vs. Crown Jewel Theft," *Forbes*, January 21, 2015, https://www.forbes.com/sites/valleyvoices/2015/01/21/the-sony-hack-and-nortels-demise-piracy-vs-crown-jewel-theft/#1efa1d54f0c9.

107 *Investigative Report on the U.S. National Security Issues*, U.S. House of Representatives.

108 Ken Hu, "Huawei Open Letter," *The Wall Street Journal*, February 5, 2011, http://online.wsj.com/public/resources/documents/Huawei20110205.pdf.

109 *Investigative Report on the U.S. National Security Issues*, U.S. House of Representatives.

110 Defending U.S. Government Communications Act, H.R. 34747, 115th Cong. (2017–2018), https://www.congress.gov/bill/115th-congress/house-bill/4747; Andrew Liptak, "A New Bill Would Ban the US Government from Using Huawei and ZTE Phones," *The Verge*, January 14, 2018, https://www.theverge.com/2018/1/14/16890110/new-bill-ban-huawei-zte-phones-tech-congress-mike-conaway-cybersecurity.

111 Nathaniel Ahrens and Yu *Zhou, China's Competitiveness: Myth, Reality, and Lessons for the United States and Japan, CASE STUDY: Lenovo* (Washington, DC: Center for Strategic and International Studies, January 2013), https://www.csis.org/analysis/china%E2%80%99s-competitiveness-lenovo.

112 Edward Wong, "University in Xi'an Opens School of Cyberengineering," *Sinosphere: Dispatches from China* (blog), *The New York Times*, January 6, 2015, https://sinosphere.blogs.nytimes.com/2015/01/06/university-in-xian-opens-school-of-cyberengineering/.

founder, was educated at China's University of Science and Technology, which was established and resourced by the CAS.[113] The CAS and its individual members have a history of coordinating with the Chinese military, including its cyber and electronic warfare operations.[114] The Chinese government, through Legend Holdings Limited, is the largest shareholder of Lenovo stock. As of June 2017, the CAS (through CAS Holdings) owned 34.83 percent of Legend and was identified as Legend's controlling shareholder.[115] In 2017, Legend had 31.48 percent ownership in Lenovo.[116] Legend, which was formed by Lenovo's founder, operates as the external investment vehicle and asset management unit of the CAS.[117] Lenovo's growth has been attributed to the economic and political support it receives from the Chinese government, including the use of state-owned intellectual property resources.[118]

Lenovo has been linked to Chinese state-led cyberespionage efforts. Lenovo products have been banned by intelligence agencies in Australia, Canada, New Zealand, the United Kingdom, and the United States (Five Eyes Countries) since the mid-2000s, when laboratories of the British intelligence agencies Military Intelligence, Section 5 and Government Communications Headquarters discovered "backdoors"[119] and vulnerable firmware in Lenovo products.[120] In 2006, after congressional inquiries into the purchase of 16,000 Lenovo computers, the U.S. Department of State said the purchased computers would be used only on unclassified systems.[121] In 2015, the U.S. Navy announced it would replace servers for its guided missile cruisers and destroyers after Lenovo acquired certain IBM server and software product lines, due to concerns that the equipment could be compromised during maintenance or remotely accessed by the Chinese government.[122] In 2016, several incidents suggested the DoD may have banned Lenovo products owing to concerns about cyber spying against Pentagon networks and concerns that the company is installing backdoors in its products for the purposes of espionage. In April 2016, an Air Force email appeared to order that Lenovo products be removed from DoD networks. This message was subsequently retracted by Air Force and Pentagon spokeswomen.[123] In October 2016, *The Washington Free Beacon* reported that the Pentagon's Joint Staff had produced an internal report warning against using Lenovo equipment.[124]

In addition, Lenovo is believed to have been complicit in installing Superfish spyware and potentially a BIOS backdoor on a number of its computer products.[125] Superfish is a preloaded software shipped with Lenovo computers that ostensibly monitored internet browser traffic to improve advertisements, but also allowed hackers to read all encrypted browser traffic, including banking transactions, passwords, emails, and instant messages. The DHS U.S.

113 "USTC Introduction," University of Science and Technology of China, About, October 14, 2016, http://en.ustc.edu.cn/about/201101/t20110113_87798.html.

114 John Costello, "Testimony before the U.S.-China Economic and Security Review Commission: Chinese Intelligence Agencies: Reform and Future," June 9, 2016, http://www.uscc.gov/sites/default/files/John%20Costello_Written%20Testimony060916.pdf.

115 Legend Holdings, "Legend Holdings Corporation, 2017 Interim Report" (Hong Kong Stock Exchange, September 14, 2017), 45, http://www.hkexnews.hk/listedco/listconews/SEHK/2017/0929/LTN201709291285.pdf.

116 Factiva Database, Dow Jones and Reuters, New York.

117 Legend Holdings, "Legend Holdings Corporation, 2017 Interim Report," 30; Factiva Database, Dow Jones and Reuters, New York.

118 Ahrens and Zhou, *China's Competitiveness*.

119 A backdoor is a means of bypassing normal authentication or encryption in a computer system, product, or embedded device. A backdoor may be a hidden part of a program, a separate program, or code in the firmware of hardware or parts of an operating system.

120 Adi Robertson, "Lenovo Reportedly Banned by MI6, CIA, and Other Spy Agencies over Fear of Chinese Hacking (Update)," *The Verge*, July 30, 2013, https://www.theverge.com/2013/7/30/4570780/lenovo-reportedly-banned-by-mi6-cia-over-chinese-hacking-fears; Christopher Joye, Paul Smith, and John Kerin, "Spy Agencies Ban Lenovo PCs on Security Concerns," *Financial Review*, July 27, 2013, accessed via WayBackMachine, https://web.archive.org/web/20130729011053/http://www.afr.com/p/technology/spy_agencies_ban_lenovo_pcs_on_security_HVgcKTHp4bIA4ulCPqC7SL; Cahal Milmo, "MI6 and MI5 'Refuse to Use Lenovo Computers' over Claims Chinese Company Makes Them Vulnerable to Hacking," *Independent*, July 29, 2013, http://www.independent.co.uk/news/uk/home-news/mi6-and-mi5-refuse-to-use-lenovo-computers-over-claims-chinese-company-makes-them-vulnerable-to-8737072.html.

121 "US Government Restricts China PCs," *BBC News*, May 19, 2006, http://news.bbc.co.uk/2/hi/americas/4997288.stm.

122 Phil Muncaster, "US Navy Looks to Dump Lenovo Servers on Security Concerns–Report," I*nfosecurity Magazine*, May 7, 2015, https://www.infosecurity-magazine.com/news/us-navy-dumps-lenovo-servers/; Megan Eckstein, "Navy Needs New Servers for Aegis Cruisers and Destroyers after Chinese Purchase of IBM Line," *USNI News*, May 5, 2015, https://news.usni.org/2015/05/05/navy-needs-new-servers-for-aegis-cruisers-and-destroyers-after-chinese-purchase-of-ibm-line.

123 Hayley Tsukayama and Dan Lamothe, "How an Email Sparked a Squabble over Chinese-Owned Lenovo's Role at Pentagon," *The Washington Post*, April 22, 2016, https://www.washingtonpost.com/business/economy/how-an-email-sparked-a-squabble-over-chinese-owned-lenovos-role-at-pentagon/2016/04/22/b1cd43d8-07ca-11e6-a12f-ea5aed7958dc_story.html.

124 Bill Gertz, "Military Warns Chinese Computer Gear Poses Cyber Spy Threat," *The Washington Free Beacon*, October 24, 2016, http://freebeacon.com/national-security/military-warns-chinese-computer-gear-poses-cyber-spy-threat/.

125 Vijay, "Lenovo PCs and Laptops Seem to Have a BIOS Level Backdoor," *TechWorm*, August 12, 2015, http://www.techworm.net/2015/08/lenovo-pcs-and-laptops-seem-to-have-a-bios-level-backdoor.html.

Computer Emergency Readiness Team issued an alert and mitigation details in response.[126] Users later discovered that Lenovo computers shipped with a rootkit-style covert installer that would reinstall unwanted software on computers after users had deleted it. In September 2017, Lenovo reached a settlement with the Federal Trade Commission over charges that the company harmed consumers. As part of the settlement, Lenovo is required to implement a comprehensive software security program for consumer software.[127] The security program will be subject to third-party audits.

TARGETING U.S. GOVERNMENT CONTRACTORS

The Chinese government and Chinese nationals have previously been linked to attempts to illegally obtain source code from U.S. ICT companies. Chinese actors, including those connected to the government, have a history of trying to obtain sensitive information about U.S. companies in order to exploit their networks, replicate their technologies, and outcompete them in the global marketplace. China-linked hacking has repeatedly targeted U.S. federal government entities and U.S. federal government contractors, including many key players in ICT contracting.[128]

In 2007, the FBI investigated Unisys after a dozen DHS computers that Unisys was supporting were compromised and significant amounts of unclassified but sensitive information was transferred to Chinese websites. It remains unknown precisely what information was removed.[129] In 2013, Bloomberg reported on China-linked hacking dating back to 2007 that targeted the North American arm of QinetiQ, a British satellite, drone, and software defense manufacturer.[130] QinetiQ supplies spy satellites, bomb disposal robots, and other products to the U.S. military. Through compromised QinetiQ networks, the hackers targeted the networks of NASA, U.S. rifle divisions, cybersecurity divisions, and databases related to the U.S. Army's Apache and Blackhawk helicopter fleet. According to *Bloomberg*, investigators attributed the attack to a group of Shanghai-based hackers nicknamed the "Comment Crew," a group linked by the cybersecurity firm Mandiant to PLA Unit 61398.[131]

China-linked hackers have also targeted RSA Security, a network security company that is a subsidiary of Dell. RSA's SecurID system is widely used by the U.S. government and its contractors for log-in security.[132] The most recent breach appears to have occurred in 2011, when a cyberattack on RSA Security led to data loss associated with RSA's SecurID system. In 2012, Gen. Keith Alexander, then director of the NSA and the head of U.S. Cyber Command, indicated in testimony before the Senate Armed Services Committee that RSA was a victim

126 Department of Homeland Security, "Lenovo Superfish Adware Vulnerable to HTTPS Spoofing," February 20, 2015, https://www.us-cert.gov/ncas/alerts/TA15-051A.

127 Federal Trade Commission, "Lenovo Settles FTC Charges It Harmed Consumers with Preinstalled Software on Its Laptops That Compromised Online Security," September 5, 2017, https://www.ftc.gov/news-events/press-releases/2017/09/lenovo-settles-ftc-charges-it-harmed-consumers-preinstalled.

128 Hanqing Chen, "A Recent History of China's Cyber Attacks on the United States," *Pacific Standard*, September 4, 2014, https://psmag.com/environment/chinas-cyber-attacks-united-states-89919; "APT1: Exposing One of China's Cyber Espionage Units," Mandiant, February 18, 2013, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf; David E. Sanger, David Barboza, and Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," *The New York Times*, February 18, 2013, http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html; Michael S. Schmidt, David E. Sanger, and Nicole Perlroth, "Chinese Hackers Pursue Key Data on U.S. Workers," *The New York Times*, July 9, 2014, http://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html; Brendan I. Koerner, "Inside the Cyberattack that Shocked the US Government," *Wired*, October 23, 2016, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

129 Mike Masnick, "FBI Investigating Unisys for Not Preventing US Gov't Computers from Getting Hacked," *Techdirt*, September 25, 2007, https://www.techdirt.com/articles/20070924/135824.shtml; Jason Mick, "Unisys Blamed for China-Connected Homeland Security Hacks," *DailyTech*, September 26, 2007, http://www.dailytech.com/Unisys+Blamed+for+ChinaConnected+Homeland+Security+Hacks/article9043.htm; Ellen Nakashima and Brian Krebs, "Contractor Blamed in DHS Data Breaches," *The Washington Post*, September 24, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/09/23/AR2007092301471.html; "Investigators: Homeland Security Computers Hacked," CNN, September 24, 2007, http://www.cnn.com/2007/US/09/24/homelandsecurity.computers/index.html.

130 Michael Riley and Ben Elgin, "China's Cyberspies Outwit Model for Bond's Q," Bloomberg, May 2, 2013, https://www.bloomberg.com/news/articles/2013-05-01/china-cyberspies-outwit-u-s-stealing-military-secrets; Michael Riley and Alex Tribou, "Hackers in China Compromise U.S. Defense Secrets," Bloomberg, May 2, 2013, https://www.bloomberg.com/graphics/infographics/hackers-in-china-compromise-us-defense-secrets.html.

131 "APT1: Exposing One of China's Cyber Espionage Units," Mandiant.

132 Elinor Mills, "China Linked to New Breaches Tied to RSA," CNet, June 6, 2011, https://www.cnet.com/news/china-linked-to-new-breaches-tied-to-rsa/.

of Chinese cyberespionage.[133] According to 2013 testimony by the executive chairman of RSA, the company detected a targeted cyberattack on its systems and recognized that product information had been extracted. RSA publicly disclosed the breach and alerted customers to help them mitigate the effects. The company took its own remediation steps, including replacing nearly all of the 40 million SecurID tokens in use.[134] Industry press reports indicate that RSA's reluctance to publicly disclose which data had been stolen during the breach may have led to breaches at other defense contractors, including Lockheed Martin, L-3 Communications, and Northrop Grumman.[135] In June 2011, Lockheed Martin confirmed that the breach it experienced was due to data stolen from RSA.[136]

In July 2013, researchers from Dell's SecureWorks unit identified hackers targeting an unnamed maker of audio-visual conference equipment.[137] The Dell researchers linked the hackers to the Chinese hacking group that breached RSA Security in 2011. Dell's researchers speculated the hackers were attempting to obtain source code of the company's products in order tap into boardroom and other high-level remote meetings. In December 2015, a former software engineer for IBM in China was arrested and charged with economic espionage and theft of trade secrets.[138] The engineer had stolen source code related to IBM's proprietary clustered file system, which facilitates faster computer performance, and attempted to share it with the PRC's National Health and Family Planning Commission.[139]

133 Kelly Jackson Higgins, "China Hacked RSA, U.S. Official Says," *Dark Reading*, March 29, 2012, https://www.darkreading.com/attacks-breaches/china-hacked-rsa-us-official-says/d/d-id/1137409; *Hearing on U.S. Strategic Command and U.S. Cyber Command, Testimony Before the Senate Armed Services* (March 27, 2012) (statement of Keith B. Alexander), 13, https://www.armed-services.senate.gov/imo/media/doc/12-19%20-%203-27-12.pdf.

134 Arthur W. Coviello, Jr., "Written Testimony before the U.S. Senate Committee on Commerce, Science & Transportation," June 25, 2013, https://www.emc.com/collateral/corporation/coviello-congressional-testimony-2013.pdf; Peter Bright, "RSA Finally Comes Clean: SecurID Is Compromised," *Ars Technica*, June 6, 2011, https://arstechnica.com/information-technology/2011/06/rsa-finally-comes-clean-securid-is-compromised/.

135 Elinor Mills, "Attack on RSA Used Zero-day Flash Exploit in Excel," CNet, April 5, 2011, https://www.cnet.com/news/attack-on-rsa-used-zero-day-flash-exploit-in-excel/; "Frequently Asked Questions about RSA SecurID: Information for RSA Customers," EMC, 2011, https://www.emc.com/collateral/guide/11455-customer-faq.pdf.

136 Christopher Drew, "Stolen Data Is Tracked to Hacking at Lockheed," *The New York Times*, June 3, 2011, http://www.nytimes.com/2011/06/04/technology/04security.html.

137 Joseph Menn, "Chinese Hackers Target Remote Conferencing Gear: Dell Researchers," Reuters, July 31, 2013, https://www.reuters.com/article/us-china-hacking/chinese-hackers-target-remote-conferencing-gear-dell-researchers-idUSBRE96U0YI20130731.

138 Nate Raymond, "Ex-IBM Employee from China Arrested in U.S. for Code Theft," Reuters, December 8, 2015, https://www.reuters.com/article/ibm-crime-china/ex-ibm-employee-from-china-arrested-in-u-s-for-code-theft-idUSL1N13X2LD20151208.

139 "Chinese National Charged for Stealing Source Code from Former Employer with Intent to Benefit Chinese Government," Department of Justice, June 14, 2016, https://www.justice.gov/opa/pr/chinese-national-charged-stealing-source-code-former-employer-intent-benefit-chinese.

Chapter 5: Closing Loopholes: Recommended SCRM Actions

Federal SCRM efforts have yet to be fully developed, and gaps in resources and processes continue to exist that allow procurement of high-risk technologies, or deployment of moderate- to low-risk technologies in ways that fail to mitigate supply chain risk. Given the budgetary challenges many federal agencies face, decisions are made on the basis of reducing cost in a way that inadvertently increases risk. Several paths could be taken to improve federal ICT supply chain security. Some involve legislative action, while others leverage federal acquisition authority.

The sections below describe four paths that should be evaluated as solutions to enhance federal ICT supply chain security, where a comprehensive solution will potentially implement more than one recommendation. Establishing a centralized leadership for SCRM, expanding legislative provisions related to SCRM, and promoting supply chain transparency are the most effective ways of improving federal ICT supply chain security, align with how industry thinks and functions, and will likely provide greater benefit and more public and private sector adoption than modifications to the role of NIST or other federal trade regulations.

ESTABLISHING CENTRALIZED LEADERSHIP FOR SCRM

Congress or the Executive Branch should (1) name the organization(s) charged with SCRM leadership, (2) provide specific resources for SCRM, and (3) encourage information sharing and consolidation of federal SCRM efforts. In the current SCRM ecosystem, responsibility for risk management is held at different levels within agencies, resulting in SCRM offices and efforts, such as those at NASA and the Departments of Energy, Commerce, and Defense, that function largely as under-resourced stovepipes, often lacking executive sponsorship or oversight, and catering to the needs and procurement policies of individual clients. Entities such as the DoD and the intelligence community maintain largely separate policies, many of which are not transparent or applicable to the broader federal government due to procurement practices and classification concerns, among other reasons. Additionally, these programs may be concerned with initial acquisition, rather than system lifecycle concerns.

Although the nature of commercial ICT means that the universe of potential suppliers serving the federal government is extremely large, SCRM analysis conducted at the GSA, Department of Energy, NASA, and Department of Commerce often covers the same set of ICT suppliers for different federal government clients. This duplication of effort is wasteful and unnecessary, and negatively affects U.S. national security posture through misspent resources and inconsistent activities. Congress or the Executive Branch could establish centralized leadership, as well as a function, to carry out baseline SCRM analysis for the entire federal government, freeing individual agencies to focus on unique suppliers and technologies and how the identified risks impact their programs. This entity would have to be resourced and staffed appropriately, and tasked with vetting to a prescribed level the suppliers and value-added resellers of products entering federal ICT networks.

The OMB should assign this authority—through modifications to Circular A-130—to the GSA, the DHS, or another federal agency that is often tasked with shared services. The GSA, which is already responsible for vetting and managing the federal government's relationship with more than 30,000 suppliers, would be a logical center of action for this effort. Given its government-wide procurement and acquisition mission, the GSA is capable of deciding what categories of risk this baseline level of analysis should include and what level of detail the analysis should pursue. It would be wise to cast as wide a net as possible, including both technical and security risks, as well as market and business risks. Funding such a venture to the point where it could create comprehensive and authoritative information would reduce the burden for agency-specific SCRM and enable agencies to build from the same foundation, focusing their efforts on particular configurations and implementation situations. Funding for this entity could include seed money as well as a cost-reimbursable model with the collaborating agencies.

However, basing a centralized SCRM effort in the GSA could present challenges. The GSA's mission is negotiating the best deal for the federal government in any procurement. Additionally, the GSA often contracts

with value-added resellers such as Mythics, DLT Solutions, Immix Group, Carahsoft, and CDW-G rather than with original equipment manufacturers (OEMs). There have been instances of OEMs (e.g., Oracle in September 2016) abandoning the GSA Schedule Contracts[140] because the effort to secure and maintain the contracts outweighed the benefits.[141] Dealing with value-added resellers rather than OEMs introduces additional risk into the federal ICT supply chain. Patrick Finn, a former senior vice president for Cisco, told Federal News Radio, "It's not uncommon for an OEM to be contacted by disgruntled customers who procured through GSA only to find out that the product was gray market or, worse, counterfeit."[142] Thus, placing SCRM for federal ICT in the hands of the GSA or any other federal agency could require not only financial and policy shifts but also cultural ones for both the government and industry. Financial cost is an element of SCRM analysis, but it should be weighed in context with security considerations.

Sharing SCRM information across the government must be done in an effective and transparent manner. The Department of Veterans Affairs (VA) has created the publicly accessible One-VA Technical Reference Module (TRM), which provides detailed information on technical risk assessments conducted by the One-VA TRM team, along with public decisions about the VA's investment or divestment in certain technologies. The TRM includes a public access site that provides TRM content, a VA internal access site that allows users to make inquiries and request technology assessments, and a TRM team collaboration site, which allows content authoring and Wiki-based development that can be pushed to published sites.[143] Users of the TRM can see when a technology was last assessed, what findings were recorded, and what actions and policies VA leadership has recommended in response to the TRM team's findings. Using a similar portal for SCRM, with distinct levels of public and government-only access, would be valuable to all federal SCRM efforts; it would prevent duplication of effort, save time, and enable agency-specific assessments to build from a common foundation and share their risk mitigation strategies. Additionally, by leveraging technology the government-wide sharing would be able to scale and sustain a robust program for all collaborating agencies.

EXPANDING THE WOLF PROVISION

Congress should expand legislative actions that address risk linked to the nature of an ICT manufacturer as well as the manufacturer's location. The Wolf Provision, or Section 516 (subsequently 515) of the 2013 Consolidated and Further Continuing Appropriations Act, is one example. This provision was added by then U.S. Representative Frank Wolf (R-VA), who chaired the House subcommittee that oversees the Departments of Commerce and Justice, NASA, and the National Science Foundation. Initially introduced in 2013, Section 516 prevented the Departments of Commerce and Justice, NASA, and the National Science Foundation from acquiring IT without first conducting a risk assessment. If the IT system was "produced, manufactured or assembled by one or more entities that are owned, directed or subsidized by the People's Republic of China" and the federal entity still wished to purchase it, then the entity had to explain to Congress why the acquisition was in the national interest of the United States.[144]

Although the Wolf Provision was criticized by industry and considered too specifically anti-China, the language of the original provision acknowledged that subjecting products to additional scrutiny purely on the basis of geographic location is not an effective course of action, especially when it comes to global ICT supply chains. The original call for scrutiny of products "produced, manufactured or assembled … by entities that are owned, directed or subsidized by the People's Republic of China," makes clear that the potential for risk does not depend solely on the manufacturing or assembly location of a product but rather on the nature of the entity overseeing production. The language of the provision was modified in 2014, and the current provision (now in Section 515 of the Appropriations Act) no longer specifically mentions China. Instead, it includes language drawn from the NIST publication FIPS 199, which requires risk assessments for high-impact or moderate-impact information

140 GSA Schedule Contracts, also known as GSA Schedules or Federal Supply Schedules, are indefinite delivery, indefinite quantity, long-term contracts under the GSA's Multiple Award Schedule Program.

141 Jason Miller, "Oracle to Leave GSA Schedule: A Signal of Broader Change?" *Federal News Radio*, September 26, 2016, https://federalnewsradio.com/reporters-notebook-jason-miller/2016/09/oracle-leave-gsa-schedule-signal-broader-change/.

142 Miller, "Oracle to Leave GSA Schedule."

143 Paul Tibbits, "DoD-VA Collaboration to Develop a Single Electronic Health Record: SOA as a Design Pattern," July 14, 2011, http://www.omg.org/news/meetings/workshops/SOA-HC/presentations-2011/14_FS-1_Tibbits.pdf.

144 Consolidated and Further Continuing Appropriations Act, 2013, H.R. 933, 113th Cong. (2013–2014), https://www.congress.gov/bill/113th-congress/house-bill/933/text.

systems. The current provision still applies only to the Departments of Commerce and Justice, NASA, and the National Science Foundation.[145]

Currently, no federal entities have all-encompassing risk assessment programs, nor are they directed to do so or be held accountable. The programs that do exist are not adequately resourced for effective implementation, and the fact that each agency interprets the requirements for itself means that SCRM practices can vary within—and between—federal agencies. Along with modifications to policy—such as Circular A-130—Congress should tie policy revisions to a funding strategy that ensures federal agencies take action in ways that are auditable. One recommendation is to expand the Wolf Provision, or Section 515 of the Consolidated and Further Continuing Appropriations Act, to apply to all federal agencies and entities. Another is to tie the SCRM requirements of this regulation to agency funding for the Modernizing Government Technology Act of 2017 in ways that require a SCRM program review for new ICT investments and modernization efforts. One improvement to the provision would be to require agencies to annually present information about (1) their established SCRM program, (2) the activities that have taken place within that program, and (3) the mitigations used. These annual reports will help build a best practices library for all federal government entities, increasing information sharing and awareness of evolving risks.

Another option is to modify the language in the Wolf Provision to direct extra scrutiny at products "produced, manufactured or assembled … by entities that are owned, directed or subsidized by" nation states or entities known to pose a potential supply chain or intelligence threat to the United States. These nation states or entities could include members of the existing Sensitive Foreign Nations Control List, the Office of the United States Trade Representative's Special 301 Report Priority Watch List, or some appropriate combination of the two.[146] This type of language would direct appropriate scrutiny at products produced by entities linked to the Chinese government, but would not place significant burden on ICT suppliers sourcing from other suppliers that may have some production facilities in China.

PROMOTING SUPPLY CHAIN TRANSPARENCY

Congress should encourage transparency and accountability for supply chains. Although this report addresses supply chains that intersect China, those are not the only sources of risk. The sheer magnitude of China's influence as a supplier and manufacturer, combined with sometimes undisclosed links between the Chinese government and Chinese firms, creates risk in federal ICT procurement. Requiring federal ICT suppliers to publish or make available information on their supply chain would increase the ability of the federal government to source responsibly and securely, and to respond to breaches in an efficient manner. The federal acquisition community could also be required to build supply chain transparency requirements or disclosures into ICT procurements for first- and second-tier suppliers, and then require that sub-tiers have this included in their flow-down clauses. Rather than seeking supply chain information from a company after an incident, the federal government and its industry partners would already have that information on hand. This information would allow the government to architect federal information systems accordingly, implement risk mitigation strategies as necessary, and trace potential weaknesses back to individual components and suppliers.

In testimony before the House Subcommittee on Communications and Technology in May 2013, Mark L. Goldstein, GAO director of physical infrastructure issues, reviewed findings from a GAO report regarding measures the governments of Australia, India, and the United Kingdom take to secure their ICT infrastructures.[147] India's licensing requirements include explicit supply chain measures such as requiring telecommunications service providers to keep a record of the supply chain for their hardware and software, and requiring suppliers to allow providers or government entities to inspect the supply chain. In the event of a security breach or an act of intentional omission, the Indian government can cancel the license of the provider and blacklist the vendor that supplied the

145 Consolidated Appropriations Act, 2017, H.R. 244, 115th Cong. (2017–2018), https://www.congress.gov/bill/115th-congress/house-bill/244/text.

146 "Attachment G Sensitive Foreign Nations Control," Department of Energy, 2014, https://energy.gov/sites/prod/files/2014/08/f18/alliance_partvII-g.pdf; Office of the United States Trade Representative, 2017 Special 301 Report (Washington, DC: Office of the United States Trade Representative, 2017), https://ustr.gov/sites/default/files/301/2017%20Special%20301%20Report%20FINAL.PDF.

147 *Telecommunications Networks: Addressing Potential Security Risks of Foreign-Manufactured Equipment, Testimony Before the House Subcommittee on Communications and Technology, Committee on Energy and Commerce* (May 21, 2013) (statement by Mark L. Goldstein), https://www.gao.gov/assets/660/654763.pdf.

hardware or software that caused the security breach.[148] This policy is similar to Section 806 authorities incorporated into the Defense Federal Acquisition Regulation Supplement (DFARS) as a final rule in October 2015.[149] Pursuing similar policies, or requiring federal contractors to provide supply chain information as part of federal contract requirements, would provide an additional layer of SCRM security when the program requires this level of rigor.

Dodd-Frank Limitations Are Future SCRM Lessons

There are challenges in significantly improving supply chain transparency, and important lessons can be learned from the experience of Section 1502 of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, which aimed to reduce violence in the Democratic Republic of the Congo by limiting U.S. procurement from actors fueling conflict in the DRC. In addition to other consumer protection provisions, Section 1502 and the ensuing Securities and Exchange Commission (SEC) rules require some companies to document the use in their products of "conflict minerals" through SEC Specialized Disclosure (SD) filings and Conflict Mineral Reports.[150]

The corporate responsibility supplier lists issued by HP, Dell, and Microsoft provide information on the first tier of the federal ICT supply chain, but the SD filings and Conflict Mineral Reports provide information on the deepest tier, the ultimate source point of the raw material a vendor is using for its ICT products. Since the passage of Dodd-Frank Section 1502 and the publication of related SEC rules, companies have filed four rounds of SD filings with the SEC and reportedly invested four years in further investigating and performing due diligence on their supply chains. And yet failings and inconsistencies remain, highlighting the scope of the challenge.

The transparency introduced by Section 1502 and the SEC rules has forced companies to diligently investigate their own suppliers, many for the first time. The policy has also raised awareness of what responsible supply chain management and responsible sourcing entail. Early on, some companies chose not to source from central Africa as a way of avoiding conflict minerals, failing to realize that global supply chains mean that conflict minerals can end up in smelters in Belgium, China, Morocco, or the United Arab Emirates. This has clear parallels to global ICT supply chains, where components may pass through several countries before being incorporated into a final product.

As Dodd-Frank made clear, the threat to U.S. national security was not minerals sourced from the DRC and adjoining countries, but rather minerals sourced from mines controlled by parties to the DRC conflict. To scope this outward, the supply chain threat to U.S. national security is not merely from products manufactured in China, or even products manufactured by Chinese businesses, but rather from products produced, manufactured, or assembled by entities that are owned, directed, or subsidized by nation states or entities known to pose a potential supply chain or intelligence threat to the United States, of which China is one.

Recommendations for improving supply chain transparency with respect to conflict minerals are applicable to supply chain transparency more generally.[151] When scoped out to ICT supply chains, new reporting requirements could require companies to note the location of their suppliers' manufacturing centers, and to identify which manufacturing centers are located in nation states known to pose a potential supply chain or intelligence threat to the United States. If a company cannot identify its suppliers' manufacturing locations, or if the location it reports appear inaccurate, it could be a warning sign that their SCRM program is not sufficient to protect the security concerns of the U.S. government.

148 *Telecommunications Networks* (Goldstein).

149 Susan Borschel, "New Department of Defense Requirements Relating to Supply Chain Risk," *Government Contracting Insights*, November 13, 2015, http://govcon.mofo.com/national-security/new-department-of-defense-requirements-supply-chain-risk/.

150 Conflict minerals are defined by U.S. legislation and SEC rules as the four metals tantalum, tin, tungsten, and gold. Tantalum, tin, and tungsten are the derivatives of the minerals columbite-tantalite (coltan), cassiterite, and wolframite, respectively. Many of these metals are sourced from the Democratic Republic of the Congo or adjoining countries. The most common conflict minerals are casserite (tin), coltan (tantalum), wolframite (tungsten), and gold, which are often collectively termed "3TG."

151 Jeff Schwartz, "The Conflict Minerals Experiment," *Harvard Business Law Review 6* (January 2015), https://ssrn.com/abstract=2548267 or http://dx.doi.org/10.2139/ssrn.2548267; *Testimony Before the House Subcommittee on Monetary Policy and Trade, Committee on Financial Services* (November 17, 2015) (statement by Jeff Schwartz), https://financialservices.house.gov/uploadedfiles/hhrg-114-ba19-wstate-jschwartz-20151117.pdf.

UTILIZING FEDERAL ACQUISITION AUTHORITIES

The final recommendation to enhance SCRM is to use the purchasing power of the U.S. government to require commercial suppliers to meet certain cybersecurity and SCRM standards to be eligible for federal contracts.[152] This option would make SCRM issues a priority for all industry partners interested in competing for government contracts, raising their level of security before they even have access to sensitive federal information. Increasing the security posture of entities before they become a target could help them defend themselves, and the federal government, against attacks from actors linked to China.

Federal contracts could use acquisition methods, including contract clauses and flow-down requirements, to require contractors and subcontractors to meet such standards. The federal government must be clear about the risk concerns and thresholds so that industry can clearly understand, based on each program, where to include SCRM investments. Although a minimum level of SCRM should be documented, not every procurement will identically use a product or service. A strict and inflexible requirement for every acquisition and supplier to undergo the maximum level of SCRM activities will be costly and unworkable.

One example of this approach is DFARS regulations on unclassified controlled technical information and controlled unclassified information, categories of information that are considered sensitive but are not classified and regulated by the federal government. These regulations require contractors to implement specific security measures in accordance with NIST SP 800-171, including access control, training, system audit records to monitor system activity, media protection and disposal, and other requirements. These measures are a necessary step, but may not mitigate the risk posed by ICT components produced in China or by entities linked to the Chinese government. NIST SP 800-171 took effect on December 13, 2017, for the DoD, the GSA, and NASA.[153]

Meanwhile, through their joint authority, the DoD, the GSA, and NASA are proposing a similar Federal Acquisition Regulation clause for contractors that handle, possess, use, share, or receive controlled unclassified information for other federal agencies.[154] This rule would have a similar effect as the DFARS and is an example of another way NIST recommendations can become obligatory.

152 Robert S. Metzger, "Threats to the Supply Chain: Extending Federal Cybersecurity Safeguards to the Commercial Sector," Bloomberg Law, June 8, 2015, https://www.bna.com/threats-supply-chain-n17179927448.

153 Matt Kozloski, "Everything You Need to Know about NIST 800-171," Kelser, December 16, 2016, https://inbound.kelsercorp.com/blog/everything-you-need-to-know-about-nist-800-171.

154 Undersecretary of Defense for Acquisition, Tech. and Logistics, "Open FAR Cases as of 10/31/2017," Department of Defense, accessed October 31, 2017, http://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf; "Federal Acquisition Regulation (FAR); FAR Case 2017-016, Controlled Unclassified Information (CUI)," Office of Information and Regulatory Affairs, Office of Management and Budget, accessed October 31, 2017, https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201704&RIN=9000-AN56.

Chapter 6: Future Considerations

As stated at the beginning of this report, the attacks on U.S. federal ICT networks will only grow as the attack vectors—and the speed with which they can be reached—increase.

As the U.S. government develops enhanced SCRM policies and regulations, it is imperative to understand—and have a strategy to address—the risk developing technologies may pose to federal ICT systems. The Chinese government and Chinese companies have developed joint strategies to influence future developments to the advantage of Chinese ICT products. China's role in setting international technology standards is likely to increase, and similar strategies are likely to be used in the future in fields beyond ICT, such as pharmaceuticals, biotechnology, medical technology, nanotechnology, virtual reality, and artificial intelligence. With China's focus on proactive measures, the United States should adopt the same forward-leaning posture focused on security.

Increasingly, the importance of an ICT component's physical structure pales in comparison with the firmware and software operating within in it. In 2016, researchers from Red Balloon Security identified vulnerabilities that allowed hackers to surveil and manipulate users by hacking the embedded firmware of computer monitors.[155] In 2017, researchers uncovered vulnerabilities in HP, Dell, and Lexmark printers that allowed attackers to steal passwords, shut down printers, and even reroute print jobs.[156] The mid-2017 CCleaner supply chain attack, in which hackers accessed the code development structure of Piriform in order to install malware into the company's Windows utility product, typifies the types of threats federal ICT systems will continue to face. Over 2.2 million users downloaded CCleaner and unwittingly downloaded the hacker's embedded malware at the same time. This malware compromised 40 international technology firms, 51 international banks, and at least 540 computers connected to various governments.[157] Firms targeted by the hackers included many within the federal ICT ecosystem, including Cisco, Google (Gmail), Microsoft, Intel, Samsung, Sony, HTC, VMware, Vodafone, Epson, and Oracle.[158] The federal government's ability to identify risks, to protect federal information systems, and to respond to and recover from attacks and breaches hinges on developing a comprehensive understanding of the supply chain risk.

Other aspects of supply chain risk depend on technologies that are not yet developed or deployed, such as 5G mobile network technology, which is expected to start deploying in 2020. 5G is important for subsequent developments in virtual reality, artificial intelligence, and seamless integration of the Internet of Things.[159] The full deployment of 5G networks is expected to dramatically expand the number of connected devices, reduce network energy use, and decrease end-to-end round-trip delay (latency[160]) to under one millisecond.[161] Although the finalization of 5G

155 Franceschi-Bicchierai, "Hackers Could Break into Your Monitor."

156 Tom Spring, "Flaws Found in Popular Printer Models," *Threat Post*, January 31, 2017, https://threatpost.com/flaws-found-in-popular-printer-models/123488/.

157 Lucian Constantin, "Researchers Link CCleaner Hack to Cyberespionage Group," *Motherboard*, September 21, 2017, https://motherboard.vice.com/en_us/article/7xkxba/researchers-link-ccleaner-hack-to-cyberespionage-group.

158 India Ashok, "CCleaner Hack: Chinese Hacker Group Axiom May Have Carried out Attack to Target Major Tech Giants," *International Business Times*, September 21, 2017, http://www.ibtimes.co.uk/ccleaner-hack-chinese-hacker-group-axiom-may-have-carried-out-attack-target-major-tech-giants-1640208; Catalin Cimpanu, "Avast Publishes Full List of Companies Affected by CCleaner Second-Stage Malware," *Bleeping Computer*, September 25, 2017, https://www.bleepingcomputer.com/news/security/avast-publishes-full-list-of-companies-affected-by-ccleaner-second-stage-malware/; Dan Goodin, "CCleaner Backdoor Infecting Millions Delivered Mystery Payload to 40 PCs," *Ars Technica*, September 25, 2017, https://arstechnica.com/information-technology/2017/09/ccleaner-backdoor-infecting-millions-delivered-mystery-payload-to-40-pcs/.

159 Sebastian Moss, "ITU and Huawei Call for Government-backed Broadband Investment," Data Center Dynamics, October 7, 2016, http://www.datacenterdynamics.com/content-tracks/core-edge/itu-and-huawei-call-for-government-backed-broadband-investment/97066.fullarticle.

160 Latency refers to the delay before a transfer of data begins following an instruction for its transfer. Decreasing latency to under one millisecond is seen as vital to successfully developing safe self-driving vehicles and producing virtual reality programs that can deliver data at a rate that feels near-instantaneous to humans.

161 Jo Best, "The Race to 5G: Inside the Fight for the Future of Mobile as We Know It," TechRepublic, https://www.techrepublic.com/article/does-the-world-really-need-5g/.

standards may be years away, Chinese entities (specifically Huawei and ZTE) have made large strides in patenting ICT innovations, so China could emerge as an industry leader in this technology.[162]

In 2016, the United States ranked first in patent filings for the 39th year in a row.[163] However, China's efforts to expand its ownership of IP are increasing; if this trend continues, China could overtake the United States in two years as the largest user of the international Patent Cooperation Treaty system. According to data from the World Intellectual Property Organization, Huawei and ZTE (along with Qualcomm) have been the top three patent filers each year since 2012.[164]

It is difficult to use patent and other IP data as a measure of a country's innovation because of differences in the policies of national patent offices and the inherent challenge of weighing the influence of any one IP application. It is also difficult to ascertain in advance which IP claims are essential to standards and which will win out when subjected to litigation. The Center for International and Strategic Studies argues that context is necessary when using patents to measure China's innovation.[165] The National Patent Development Strategy of China's State Intellectual Property Office explicitly equates patent generation with innovation. To encourage companies to file patents, the Chinese government offers incentives such as cash bonuses, subsidies, and lower corporate income taxes. This strategy might encourage quantity over quality, so that some State Intellectual Property Office patents are awarded for incremental innovations and design modifications rather than dramatic innovations.

Moreover, large increases in domestic patent filings in China have not translated into large increases in the number of triadic patents, which are patents filed jointly in the three largest global technology markets: the Japanese Patent Office, the U.S. Patent and Trade Office, and the European Patent Office. The Center for International and Strategic Studies notes, "While China now processes the greatest number of domestic patent applications annually, these patents do not hold up under the more stringent requirements of the international patent system."[166] Additionally, Chinese patent applications are not spread widely among Chinese firms but rather are concentrated in the hands of government-backed ICT firms such as Huawei and ZTE.

The Chinese government and Chinese firms are hoping for a larger stake in the new 5G developments than they had in 3G and 4G-LTE.[167] Of the 4,123 patents that ZTE applied for in 2016, more than 1,500 are 5G-related.[168] Huawei's 5G research dates to 2009 and includes advances in polar coding and network splicing routers. Huawei has also bought technology patents from Sharp, IBM, Siemens, Harris Corporation, and other U.S., Japanese, and European companies. These patent acquisitions focus on communication technologies such as the Session Initiation Protocol.[169]

A March 2017 report by LexInnova laid out the major players in the 5G network technology IP landscape.[170] **Exhibit 4** shows share of 4G-LTE and 5G IP among top firms. Qualcomm, Nokia, InterDigital, Ericsson, Intel, and Huawei are the top six firms for 5G IP. Qualcomm, Samsung, Intel, Ericsson, Nokia, and LG were the top six firms for

162 Ben Sin, "How Huawei Is Leading 5G Development," *Forbes*, April 28, 2017, https://www.forbes.com/sites/bensin/2017/04/28/what-is-5g-and-whos-leading-the-way-in-development/#1d015f0e2691.

163 World Intellectual Property Organization, "Record Year for International Patent Applications in 2016; Strong Demand Also for Trademark and Industrial Design Protection," press release, March 15, 2017, http://www.wipo.int/pressroom/en/articles/2017/article_0002.html.

164 World Intellectual Property Organization, "U.S. Extends Lead in International Patent and Trademark Filings," press release, March 16, 2016, http://www.wipo.int/pressroom/en/articles/2016/article_0002.html; World Intellectual Property Organization, "Telecoms Firms Lead WIPO International Patent Filings," press release, March 19, 2015, http://www.wipo.int/pressroom/en/articles/2015/article_0004.html; World Intellectual Property Organization, "US and China Drive International Patent Filing Growth in Record-Setting Year," press release, March 13, 2014, http://www.wipo.int/pressroom/en/articles/2014/article_0002.html; World Intellectual Property Organization, "Strong Growth in Demand for Intellectual Property Rights in 2012," press release, March 19, 2013, http://www.wipo.int/pressroom/en/articles/2013/article_0006.html.

165 China Power Team, "Are Patents Indicative of Chinese Innovation?" China Power, February 15, 2016, updated August 11, 2017, https://chinapower.csis.org/patents/.

166 China Power Team, "Are Patents Indicative of Chinese Innovation?"

167 4G-LTE, or long-term evolution, is a telecommunication standard for high-speed wireless communication for mobile devices and data terminals.

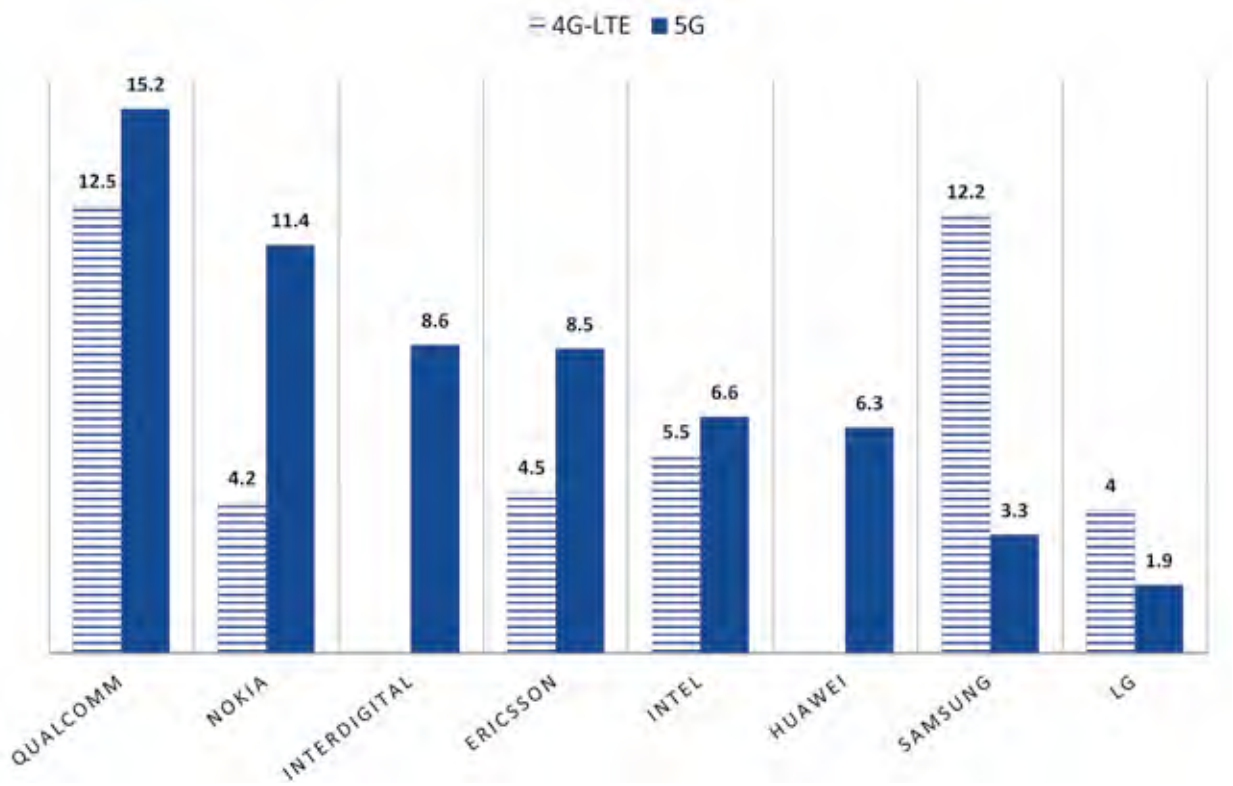
168 Saleha Riaz, "ZTE, Huawei Top Patent Application Table in 2016," *Mobile World Live*, March 16, 2017, https://www.mobileworldlive.com/featured-content/top-three/zte-huawei-top-patent-application-table-in-2016/.

169 Jack Ellis, "A Peek Inside Huawei's Shopping Basket Reveals How Patent Purchases Further Its Expansion Plans," IAM, May 7, 2015, http://www.iam-media.com/Blog/Detail.aspx?g=0351e5a1-3675-43a9-a552-7c8206af6be3.

170 "5G Mobile Network Technology: Patent Landscape Analysis," LexInnova, March 15, 2017, http://www.lex-innova.com/resources-reports/?id=67.

4G-LTE IP. Many of the top firms from 4G-LTE development remain competitive in the 5G sphere, with Qualcomm continuing to lead the group, and Nokia, Ericsson, and Intel increasing their share of relevant IP rights in 5G with respect to 4G-LTE. Although Samsung was a close second to Qualcomm in 4G-LTE innovation, it has fallen to 10th in 5G IP, according to the LexInnova data. LG has similarly struggled, losing influence in 5G innovation to its competitors. Newly important players include InterDigital (a nonparticipating U.S. entity that owns IP but does not produce products) and Huawei.

Exhibit 4
Percent Share 4G-LTE and 5G Wireless Network IP Rights by Firm



Sources: LexInnova, iRunway, Jefferies.

According to the LexInnova data, Huawei may control as much as 6.3 percent of critical 5G mobile network technology IP, a shift from its lack of influence in 4G-LTE. All Chinese entities together (including contributions from Huawei, ZTE, the China Academy of Telecommunications Technology, Zhejiang University, and Lenovo Group) control 9.8 percent of the IP LexInnova deemed critical to the 5G standard. Chinese firms have the largest presence in the Radio Front End/Radio Access Network category, where Huawei has 41 patents, China Academy of Telecommunications Technology has 14, ZTE has 11, and Zhejiang University has 10. In the area of Modulation/Waveforms, Huawei has 27 patents, while Lenovo Group has 7. In the area of Core Packet Networking Technologies, Huawei has 24 patents and ZTE has 8. However, Chinese entities still lag behind ICT powerhouses such as Ericsson, Qualcomm, and Nokia, which represent the bulk of 5G-related patent holders.[171] The LexInnova report notes that the presence of Chinese entities among the top IP assignees may indicate that China's 5G deployment timeline is similar to that of the United States.

The creation of 5G standards is divided into two phases. Phase 1 will be finalized by the end of 2017; it is a soft transition phase to 5G that involves backward compatibility with 4G-LTE to protect legacy investments. Phase 2 will be finalized in mid-2018 and will introduce significant changes. Key decisions on these standards will be made in international organizations such as the International Telecommunication Union (ITU) and the Third Generation Partnership Project (3GPP). The ITU is a specialized agency of the United Nations responsible for ICT issues; the 3GPP is a collaborative organization among telecommunications associations. In both arenas, China has sought

171 Guy Daniels, "If You Thought Patents Got Ugly with LTE, Just Wait until 5G," *Telecom TV*, http://www.telecomtv.com/articles/5g/if-you-thought-patents-got-ugly-with-lte-just-wait-until-5g-13458/.

leadership positions to increase its influence. In the 3GPP, China has been represented by members of Huawei and China Mobile. In October 2014, Houlin Zhao was elected secretary general of the ITU.[172] His four-year term began January 1, 2015, and concludes at the end of 2018. In October 2016, Huawei's Site Energy Efficiency proposal was approved by the ITU.[173] The 3GPP has also accepted Huawei-backed polar code as the coding method for the control channel for 5G Phase 1,[174] and Chinese companies have several proposals in play for Phase 2.[175]

172 "Biography–Houlin Zhao," International Telecommunication Union, 2017, http://www.itu.int/en/osg/Pages/biography-zhao.aspx; Xinhua, "China's Zhao Houlin Elected as Secretary-General of ITU," *China Daily USA*, October 23, 2014, http://usa.chinadaily.com.cn/world/2014-10/23/content_18791007.htm.

173 "Huawei's SEE Becomes International Standard after ITU Approval," Huawei, December 5, 2016, http://www.huawei.com/en/news/2016/12/Huawei-SEE-International-Standard-ITU.

174 Louise Lucas and Nic Fildes, "Huawei Aims to Help Set 5G Standards," *Financial Times*, November 29, 2016, https://www.ft.com/content/f84f968c-b45c-11e6-961e-a1acd97f622d.

175 Edison Lee and Timothy Chau, "Telecom Services: The Geopolitics of 5G and IoT," Jefferies Hong Kong Limited, September 14, 2017. http://pdf.zacks.com/pdf/JY/H5194437.PDF.

Conclusions

It is unlikely that political or economic shifts will push global ICT manufacturers to dramatically reduce their operations in China or their partnerships with Chinese firms. A national strategy is needed for supply chain risk management of U.S. ICT, and it must include supporting policies so that U.S. security posture is forward-leaning, rather than reactive and based on incident response.

To successfully manage risks associated with Chinese-made products and services and the participation of Chinese companies in ICT supply chains, the U.S. government should:

- ***Establish Centralized Leadership for SCRM***: Threats to U.S. national security posed by state-directed or state-backed adversaries targeting U.S. federal ICT systems will continue, and China's role is in global ICT supply chains is unlikely to change in the near future. In a constrained resource environment, the federal government will need to have a strategy that focuses policy on those threats and vulnerabilities that have the greatest likelihood of occurrence. Establishing a technology-enabled shared SCRM services capability that all federal agencies can access is likely the most cost-effective and impactful means for tackling this evolving threat. A centralized entity for SCRM would need executive-level sponsorship, to be resourced and staffed appropriately and tasked with vetting to a prescribed level the suppliers and value-added resellers of products entering the federal IT network. This entity's work should be unclassified, but the entity should have a relationship with the intelligence community to ensure collaboration and information sharing.
- ***Embrace an Adaptive SCRM Process***: Federal ICT modernization efforts mean that new products entering the federal information systems and NSS have increasingly complex and globalized supply chains, many of which include commercial suppliers that source from China. These supply chains will change over time as companies develop new technologies and partner with new suppliers, and effective SCRM policies must be able to adapt as well. Policymakers must empower rather than hinder the efforts of successful collaborative entities such as NIST and keep as much discussion of the supply chain threat as possible in the unclassified public sphere.
- ***Promote Supply Chain Transparency***: The government should encourage the public exposure of primary or tier-one suppliers to federal ICT providers and should push for transparency of all suppliers where necessary for certain systems or suppliers at a particular risk or impact level. Suppliers should be required to be transparent about their relationships with entities that are owned, directed, or subsidized by nation states like China, or other entities known to pose a potential supply chain or intelligence threat to the United States. The government should have mechanisms in place and reward industry engagement with these efforts, while establishing consequences for failure to mitigate risk exposure.
- ***Prioritize SCRM throughout the Lifecycle of a Program***: The federal acquisition community should build supply chain transparency requirements or disclosures into ICT procurements from "birth to demise." Having supply chain information on hand earlier and until the end of the program will allow the government to architect federal information systems accordingly, implement risk mitigation strategies as necessary, and trace potential weaknesses back to individual components and suppliers while the program is operational.
- ***Have a Strategy and Craft Froward-Looking Policy***: Next-generation technologies and standards will have implications for U.S. national security in ways that may not be addressed by existing policies and regulations. Identifying future supply chain risks and addressing them creatively will be important to the success of federal policy efforts. Future risks will likely involve software, cloud-based infrastructures, and hyper-converged products rather than hardware. A vendor's, supplier's, or manufacturer's business alliances, investment sources, and joint R&D efforts are also sources of risk not always addressed in traditional SCRM.

Having a strategy that includes these steps will ensure that new SCRM policies can be adaptive, be collaborative, and achieve buy-in from both government and industry. Increased transparency will enhance the security of the federal ICT supply chain by enabling the federal government to source responsibly and securely, and by improving the government's ability to respond to incidents in the event of a supply chain attack, while centralization will reduce the burden facing agency-specific SCRM and allow agencies to focus their efforts on particular configurations and implementation situations. Moreover, building supply chain security into policy from the beginning will prevent costly mitigation later, and ensure that federal ICT supply chains—and the federal information systems they supply—remain secure.

Scope Note

This paper is an unclassified report on commercial supply chain vulnerabilities in U.S. federal ICT procurement linked to the People's Republic of China. The study was requested by the U.S.-China Economic and Security Review Commission and is intended as a reference for policymakers, China specialists, and supply chain professionals on how the U.S. government manages risks associated with Chinese-made products and services and the participation of Chinese companies in U.S. ICT supply chains. The research for this project covered three major connection routes between China and U.S. federal ICT supply chains and the risks those connections pose to U.S. national security. Sources used in this paper may refer to information technology, which can include computers, software, electronics, and other information distribution technologies. This paper's scope addresses the more expansive category of ICT, which encompasses audio-visual communications systems, data storage, and other integration technologies.

METHODOLOGY

This study defines "U.S. government ICT supply chains" as (1) primary suppliers, (2) tiers of suppliers that support primary suppliers by providing products and services, and (3) any entities linked to those tiered suppliers through commercial, financial, or other relevant relationships. This comprehensive definition includes supply chains that are multi-tiered, webbed relationships in addition to those that are singular or linear in nature. The greatest risk is often found in the second or third tiers of a supply chain and in indirect relationships within the chain.

The Commission requested a study that reviewed laws, regulations, and other requirements since the passage of FITARA in February 2014. The study includes detailed recommendations to minimize the risk that the Chinese government, Chinese companies, or Chinese products may pose to U.S. federal ICT supply chains. Interos supply chain risk analysts and China experts were specifically tasked by the Commission to assess—

1. China's role in the global ICT supply chain and China's participation in U.S. federal ICT supply chains, including U.S. government reliance on Chinese firms, products, and services and the risk those products and services pose to U.S. economic health and national security
2. Cases in which the Chinese government, Chinese companies, or Chinese products have been implicated in connection with U.S. supply chain vulnerabilities or exploitation
3. Current U.S. government efforts to manage risk from foreign-made products and foreign firms participating in its IT procurement, including differences between non-national-security-related and national-security-related ICT procurement
4. Points of vulnerability and loopholes in the existing U.S. federal risk management system, including prospects for future development as Chinese manufacturing, research, and development capabilities evolve

Included in this report are seven of the largest providers of enterprise IT to the U.S. federal government that are also ICT OEMs: HP, IBM, Dell, Cisco, Unisys, Microsoft, and Intel.[176] This is not to say these are the only companies with potential challenges in their supply chains, and it should be noted that none of these companies were approached as part of this report. Although all of these companies conduct some level of due diligence on their supplier base, their complete records are not publicly available.

176 "Top 25 Enterprise IT Providers," FedScoop.

SOURCES

The source material for this study is unclassified, publicly available, open source information, to include information from media, the internet, public government data, academic and industry publications, and commercial databases. For some subjects, the implications of unclassified information are highly suggestive yet inconclusive. For example, unclassified information is often insufficient to conclusively attribute ICT network intrusions and telecommunications supply chain vulnerabilities to the Chinese government, Chinese companies, or Chinese products. The analysis and attributions in this study present the best available unclassified information, with appropriate caveats when necessary.

The Chinese source material for the study came from authoritative PRC publications and authors, including government-affiliated press entities, and from the Chinese- and English-language web pages of Chinese companies, including defense providers and ICT suppliers.

Additional data used in the supply chain analysis of major U.S. federal ICT suppliers were obtained from relevant open source intelligence, including social media, free and subscription services, and other structured and unstructured data sources.

The result is a comprehensive review of the links between major U.S. federal ICT suppliers and the Chinese government, Chinese companies, and Chinese products that may pose a risk to U.S. federal ICT supply chains.

Acknowledgments

Interos Solutions would like to thank the U.S.-China Economic and Security Review Commission for its support of this research and the opportunity to present these findings. That said, we could not have produced this report without help from others. Our thanks are also due to Tara Madison, Sheila Gagen, Johanna Daproza, and other members of Vector Talent Resources for their editorial and design support.